PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 12/14 — A2

(11) International Publication Number: **WO 99/07108**

(43) International Publication Date: 11 February 1999 (11.02.99)

(21) International Application Number: PCT/FI98/00590

(22) International Filing Date: 14 July 1998 (14.07.98)

(30) Priority Data:

972980	14 July 1997 (14.07.97)	FI
981031	8 May 1998 (08.05.98)	FI

(71) Applicant *(for all designated States except US)*: NOKIA TELECOMMUNICATIONS OY [FI/FI]; Keilalahdentie 4, FIN–02150 Espoo (FI).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: EKBERG, Jan–Erik [FI/FI]; Seljatie 1 A 5, FIN–00320 Helsinki (FI). GINZBOORG, Philip [IL/FI]; Koillisväylä 17 B 15, FIN–00200 Helsinki (FI). LAITINEN, Pekka [FI/FI]; Sörnäisten rantatie 3 B 33, FIN–00530 Helsinki (FI). YLÄ–JÄÄSKI, Antti [FI/FI]; Vehkamäki 11 C 6, FIN–02180 Espoo (FI). FLYKT, Patrik [FI/FI]; Silmupolku 1 A 6, FIN–00380 Helsinki (FI). SÖDERLUND, Tom [FI/FI]; Gyldenintie 8 A 18, FIN–00200 Helsinki (FI).

(74) Agent: PATENT AGENCY COMPATENT LTD.; Teollisuuskatu 33, P.O. Box 156, FIN–00511 Helsinki (FI).

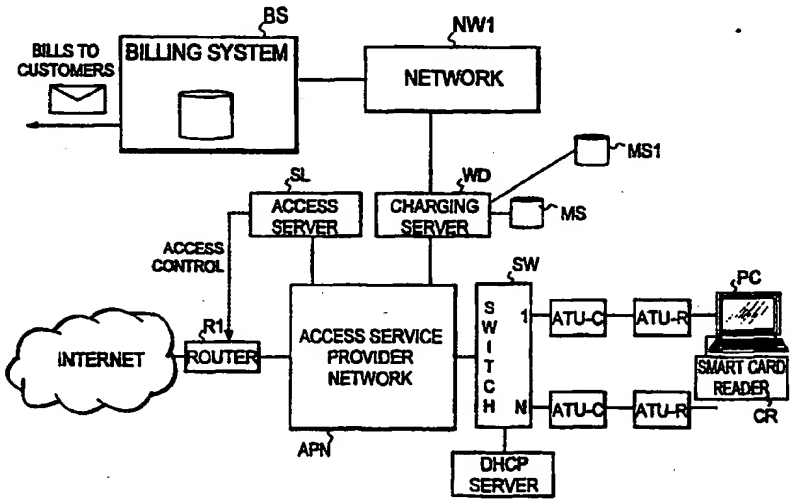
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

In English translation (filed in Finnish).

Without international search report and to be republished upon receipt of that report.

(54) Title: IMPLEMENTATION OF ACCESS SERVICE



(57) Abstract

The invention relates to the implementation of access service in a telecommunications network comprising an access network, a network providing services, and user–operated terminals (TE1... TE3, PC) connected to the access network. The access service is provided by connecting the user terminal to the network providing the services through interface elements that connect the access network to the network providing the services, and in response to the access service at least one charging record is generated for transmission to the billing means (BS) for billing the access service subscriber for the access service provided. To ensure that reliable and versatile billing can be incorporated into the system in a connectionless network, the start–up of a single access service session is indicated by generating a start–up message for charging purposes at the moment when the user connects to the access network through the terminal, charging records with a digital signature associated with the said access service session are generated and the generated signatures verified. The terminal is given access to the network providing the services, if the said messages are generated in an acceptable manner. The object generating the start–up messages can be modified according to the type of network involved.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Implementation of access service

Field of the invention

The invention is related in general to the implementation of access service in a telecommunications system, in particular to the implementation of charging in connection with access service. In this context the term 'access service' refers to a service which gives the user of a network, such as the subscriber of a telephone network or a LAN user, access to the network that provides services, for example the Internet, or to a section of the network by which the services are being provided.

Background of the invention

Optical fiber is a natural choice for the transmission medium for a trunk network because trunk connections usually require a high transmission capacity, the transmission distances are long and existing routes for cables are often available. With subscriber connections (the line between the local exchange and the subscriber), the situation is also rapidly changing because various multimedia services that require a high transmission rate will soon be commonplace for private consumers as well.

However, no major savings are foreseeable in the construction costs of networks providing broadband services in the future because the costs are mostly due to cable installation. On the one hand, it is desirable that as much optical fiber as possible would also be laid in subscriber networks, as it will obviously be needed in the future. On the other hand, the cost of refurbishing the subscriber network is extremely high, and such modernisation will take decades. Consequently, high costs constitute the main obstacle to a more widespread use of optical fiber in subscriber networks.

For the reasons listed above, more effective steps have been taken to explore the possibility of using the conventional subscriber line (twisted pair cable) for high-speed data transmission, i.e. for speeds that clearly exceed the speed of the ISDN basic connection (144 kbit/s). The present ADSL (Asymmetrical Digital Subscriber Line) and HDSL (High bit rate Digital Subscriber Line) technologies offer new prospects for high-speed data and video transmission via the telephone line to subscriber terminals.

The ADSL transmission connection is asymmetric in that the transmission rate from the network to the subscriber is significantly higher than that from the subscriber to the network. Accordingly, the ADSL technology is mainly intended for various subscriber services ("on-demand" services). The speed of an ADSL transmission from the network to the subscriber is in the order of 2 to 6 Mbit/s and from the subscriber to the network in the order of 16 to 640 kbit/s (the control channel only).

The HDSL transmission technology is used for the transmission of 2 Mbit/s digital signals in a twisted pair cable. The HDSL technology is symmetrical in the sense that the transmission speeds are identical in both directions. A single HDSL transceiver system comprises transceivers that make use of the echo cancellation technology and are inter-connected by a two-way transmission path consisting of a twisted pair cable. A HDSL transmission system may include one, two or three such transceiver systems in parallel; for two or three parallel pairs, the speed of each parallel transmission connection is less than 2 Mbit/s, being 784 kbit/s for three parallel pairs and 1168 kbit/s for two parallel pairs. International recommendations define how the signals at the 2 Mbit/s level, such as the VC-12 signals used in the SDH network or the 2048 kbit/s signals compatible with the CCITT G.703/G.704 recommendations, are transmitted in a HDSL system.

Because the aforementioned solutions only provide speeds in the order of 1 to 6 Mbit/s, steps have been taken to find a technology for the subscriber line that would permit ATM-level speeds (10 to 55 Mbit/s). The international standardisation organisation ETSI (European Telecommunications Standards Institute) is in the process of creating specifications for VDSL (Very high data rate Digital Subscriber Line) devices that would permit such speeds. The VDSL technology can be used for both symmetrical and asymmetrical connections.

The aforementioned technologies used for transmitting fast data over a twisted pair cable are known by the common acronym of xDSL. Although it is not yet possible to provide broadband services to end users by way of optical fiber, teleoperators are in a position to offer such services through the existing subscriber lines with the above-mentioned technologies. Currently ADSL appears to be the most promising technology for the implementation of broadband services and, therefore, it is used as an example of the connection technology for the provision of these services.

The ADSL Forum has defined a general network model for xDSL connections, which is illustrated in Figure 1. The device that connects to the line at the user end is called ATU-R (ADSL Transmission Unit - Remote), and the device that connects to the line at the network end (at the local exchange) is called ATU-C (ADSL Transmission Unit - Central). These devices, also known as ADSL modems (or ADSL transceivers), create an ADSL link between them. The high-speed data supplied from the ADSL connection is connected to the subscriber line in such a way that the subscriber can still use the conventional narrow-band POTS/ISDN services while at the same time having access to a high-speed data connection. These narrow- and broadband services are separated from one another using the PS filter (POTS splitter) which carries out the frequency separation of ADSL signals and narrowband signals.

The terminals TE located at the end user may be of various types, such as cable TV terminals TE1, personal computers TE2, or ISDN telephones TE3. For each terminal, the system features a service module SMi (i=1...3) that performs the functions required for terminal adaptation. Such service modules include the so-called Set-Top Boxes, PC interfaces, or LAN routers. The distribution network PDN (Premises Distribution Network) in the subscriber's premises connects the ATU-R to the service modules.

At the network end of the ADSL link the access node AN forms a concentration point for narrowband and broadband data, where the traffic from the various service systems carried via various networks converges. For example, the access node may be at the central exchange of the telephone network

The letter A in Figure 1 represents the private section of the network, B the public section network, and C the network within the subscriber's premises (the telephones naturally being inside).

The problem with a network of the type described above is how to charge the end user for access (i.e. for the use of the subscriber line) to the services offered by the service systems, such as Internet services. Preferably, charging should be based on time or the volume of transmitted data, or on both. Primarily, the problem is caused by the fact that the network can be of the connectionless type. In other words, the network does not feature messages for establishing and releasing a connection (such as SETUP and RELEASE), and so the charging cannot be carried out in the same way as in

the conventional telephone network, where it is based on connection set-up and release events. Secondly, the manufacturers of xDSL modems have not included features in their devices that would allow charging based on time or the volume of data transmitted. As a result, it is not possible to query the modems for the data required for charging.

It should be noted that if the terminal is an ISDN or ATM terminal, each session starts with a SETUP message and finishes with a RELEASE message, in which case time-based charging can be implemented using the conventional method. Consequently, the problem discussed above affects networks where the network section between the terminal and the access node, or at least the link between the terminal TE and the delivery network PDN, is connectionless. More specifically, it is possible to construct the transmission path between the terminal and the access node in such a way that the section between the access node and ATU-R is of the connection-oriented type (such as ATM-based) and the section between the ATU-R and the terminal of the connectionless type (such as an Ethernet link).

With connectionless systems that support terminal mobility, the problem is also how to charge the end user for access services. This is because the protocols that support terminal mobility (such as mobile IP, IP=Internet Protocol) do not permit classification of network users by specific criteria, such as paying customers.

With fixed terminal devices, the problem is further complicated by a situation where several customers use the same subscriber line, which makes it impossible to distinguish between users according to the line involved. Such a situation arises, for example, when the public is offered access to broadband services by placing the terminal in public premises, such as a library or shopping centre. The same problem arises when employees wish to work from home by establishing a connection only with the LAN of the employer. In this case, it is not possible to determine that the invoice for the session should be addressed to the employer instead of the user. More precisely, the system is unable to differentiate between when a user is setting up a connection as a business user (whose bills are paid by the employer) and when as a private user (who pays his or her own bills).

From now on, the term "user" will be used to refer to the individual who uses the terminal, and the term "subscriber" to refer to the organisation or individual who pays for the use of the service. A user can also be a subscriber.

Summary of the invention

The purpose of the invention is to eliminate the drawbacks described above and to provide a solution which can be used to implement an access service in a connectionless network using as simple equipment as possible to ensure that a reliable and flexible charging function can be incorporated into the system. Another objective of the invention is to provide a solution that is suitable for use both in networks that support terminal mobility and in situations when the bill is to be sent to an address other than that determined by the subscriber line or the subscriber identified by the terminal network address.

These objectives can be attained by means of the solution defined in the independent patent claims.

First of all, the idea of the invention is to use a start message to indicate the beginning of a single session when the user accesses the network. The entity that generates the start message may vary according to the system involved, and the start message can be transmitted in various ways to the elements that handle billing. Secondly, the idea is to generate, in the network, verifiable charging messages which relate to the service session initiated by said start message and which are furnished with subscriber-specific digital signatures, for example, and to allow (or disallow) access to the network depending on whether the terminal generates such charging records correctly.

This makes it possible, among other things, to restrict access rights to paying users and to distinguish between the various users of the same source address for billing purposes. If several users make use of the same subscriber line, the terminal indicates the identity of the subscriber associated with the current user for verification of the signature against the data of the correct subscriber.

The system is, in principle, such that all factors essential to data security can be easily implemented: authentication, data integrity, non-repudiation (a party to the data transmission cannot afterwards deny participation in the transaction) and privacy (an eavesdropper is unable to decipher any captured data).

A significant additional advantage of the system is that it can simultaneously carry out charging for the services used by the customer after he or she has gained access to the network providing the services, such as

the Internet. On the terminal display, the customer can simultaneously see the charging data for the connection itself as well as the services used and receive all charging data fully itemised in one periodic (e.g. monthly) bill.

The system is also capable of using charging systems that already exist (e.g. in the telephone network), and will thus not require new solutions or investments in this respect.

A brief description of the drawings

The invention and its preferred embodiments are described in more detail below, with reference to Figures 2 through 15 using examples depicted in the following drawings, where:

Figure 1 illustrates the general network model defined by the ADSL Forum;
Figure 2 shows a network environment in which the method suggested by the invention can be used;
Figures 3a and 3b show a system in accordance with the invention in operation in the network environment illustrated in Figure 2;
Figures 3c and 3d show alternatives to the systems shown in Figures 3a and 3b;
Figure 4 shows the dialog box that appears on the terminal display;
Figure 5 illustrates message exchange between the various system components;
Figure 6 illustrates, in more detail, the operations that take place between the access server and router;
Figure 7a shows the main window of the terminal display;
Figure 7b shows the bill to be sent to the customer;
Figure 7c shows the debt incurred by the user when all the required payments are not received by the charging server;
Figure 7d shows the debt incurred by the user when the clocks of the charging server and terminal are out of synchronisation;
Figure 8 shows the structure and contents of the charging record;
Figure 9a shows the structure of the terminal in the form of a functional block diagram;
Figure 9b provides a more detailed description of the structure of the CDR generator;

Figure 10 shows the structure of the charging server in the form of a functional block diagram;

Figure 11 shows the structure of the access server in the form of a functional block diagram;

Figure 12 illustrates message exchange associated with one preferred additional feature of the system;

Figure 13 illustrates message exchange between various system components when the network uses the mobile IP protocol that permits IP level mobility;

Figure 14 illustrates message exchange between various system components when the network uses the IPv6 protocol; and

Figure 15 shows one system in accordance with the invention that supports IP level mobility.

A detailed description of the invention

In the following, the operating environment of the invention is described in detail with reference to an example according to Figure 2, in which the general network model according to Figure 1 is presented in a simplified form. The network is assumed to include an operator ISP that provides Internet services and is, for the purposes hereof, called the access service provider. This example only shows one terminal which is typically a personal computer PC featuring a network interface (such as an Ethernet card) and connected via the LAN cable LC1 (for example, 10BaseT) to the ADSL modem A1 which is in turn connected via an ordinary subscriber line SL to the ADSL modem A2 located in the premises of the access service provider. As the twisted pair cables serving as subscriber lines terminate at the telephone operator exchange, the modem A2 must be located at the exchange premises in order to ensure maximum distance.

For the purposes of this example, it is assumed that the operator offering the Internet services also serves as a teleoperator. However, the POTS splitter makes it possible for the teleoperator to provide only telephone services and to rent the connection to another service provider for the provision of broadband services. Future antitrust legislation may even compel teleoperators to adopt this policy unless they themselves offer broadband services.

In the network shown in Figure 2, the network PDN located in the end-user premises is reduced to a point-to-point connection between the terminal and the access service provider. The modem A2 is connected by the LAN cable LC2 (such as 10BaseT) to the LAN switch SW of the service provider. This switch connects the various subscriber connections to the access service provider network APN, which is connected to the Internet via the router R1 serving as a gateway. The access network section of the system is denoted in Figure 2 by the symbol N1 and the external network providing the services by the symbol N2. The access network can also be regarded as that part of the network that connects the terminals to the part of the network that provides the services (thus, the router R1 may also be assumed to be part of the access network).

In this example, Ethernet frames are transmitted across an ADSL connection while the modem pair serves as a bridge between the LAN segment of the subscriber and the LAN segment of the access service provider. In reality, the LAN switch may, for example, be the Centillion 100, manufactured by Bay Network, USA, or the Catalyst 3000, manufactured by Cisco Systems, USA.

Figure 3a illustrates how the method in accordance with the invention is applied in the network environment shown in Figure 2. The end-user terminal (a personal computer) includes a smart card reader CR, and each customer is issued with a personal smart card by which the customer (subscriber) is identified. In addition, the terminal contains a program library to communicate with the smart card, as well as software that generates, at pre-defined intervals (such as once a minute) while the connection is on, a charging record complete with the user's digital signature and sends it to the network.

A charging server WD that verifies and collects the charging records generated by the terminals is connected to the network APN of the access service provider. The network may include several different charging servers, but there is, however, a dedicated charging server for each terminal. The charging server features the memory MS, such as a magnetic tape, which is used for storing all charging records accepted by the charging server. The accumulated charging records are transferred periodically to the billing system BS which is preferably an existing billing system in the public switched telephone network PSTN or, for example, a system similar to the existing

billing system but located in a broadband network. The network NW1, which is shown in general outline in the figure and through which the charging server is connected to the billing system, can thus consist of the public telephone network or a packet or data network. With the increasing number of systems used for charging for Internet services, this type of billing system (located in the Internet) may also be employed for these purposes. This alternative is denoted by the dashed line in the figure. The charging server may also be directly connected to the billing system. Before their transfer to the billing system, the charging records can be temporarily saved in the mass memory device MS1, which serves as an intermediate storage facility and whose purpose is described later.

Additionally, an access server SL is connected to the network of the access service provider. The task of the access server SL is to open and close Internet connections by controlling the router/concentrator R1, which functions as the connecting component between the access network and the network that provides the services.

In a preferable embodiment, the system includes a known DHCP server (Dynamic Host Configuration Protocol) for dynamic allocation of IP addresses to terminals. In dynamic address allocation, the address is returned to the pool of addresses to be allocated once the connection is terminated or a pre-determined "rental period" of the address expires. (A description of DHCP is provided in *Dynamic Host Configuration Protocol*, RFC-1541, October 27, 1993, by R. Droms.)

The charging and access servers are preferably located in the premises of the access service provider, and they need not be physically separate but can be integrated into the same unit. The charging server, in particular, can be located on the Internet side of the system, especially if the charging server is owned by a separate organisation which offers billing services to several access service providers. Logically, the location of the charging server is of little importance, but in practice the selection of the location is influenced by factors such as the following. First, it is advisable to install the charging server in or near the public telephone network to ensure easy access to the existing billing system of the telephone network. For the sake of efficiency, it is essential that the connection between the terminal and the charging server is as fast as possible and that any delay is easily controlled (which is not always the case, if the charging server is far inside the

Internet). Since the system is also designed to provide a local service (in a geographically limited area) in the sense that the customers are billed for the services, for example, once a month, it does not make sense to have the charging server far away from the customers.

The POTS splitter is omitted in Figures 2 and 3a (cf. Figure 1) because the splitter can also be integrated with the ATU.

Figure 3b shows an alternative system which is otherwise similar to the system in Figure 3a except that between the access service provider network APN and the switch SW there is the router R2 which, in this case, is the router that is controlled by the access server. The access control point can thus be located at either router. The router R2 routes the traffic from the terminals either to the servers located in the access service provider network or to the router R1. It is also possible to have access control points at both routers. Such a situation may arise, for example, when some of the services are located in the access network and the rest elsewhere.

Figures 3c and 3d show two other alternative networks. In the case illustrated in Figure 3c, several individual access service providers are connected to the shared router R1, which is connected via a separate access network ACN to the router controlled by the access server. In the case illustrated in Figure 3d, the access service providers have their own routers (not shown), and so their networks are directly connected to the access network.

According to one preferred embodiment of the invention, the transmission paths between both the access server and the access control point and between the access server and the charging server are secured to ensure the privacy of the transmitted data. This can be accomplished either physically by using a dedicated transfer medium inaccessible to others between the elements involved (point-to-point connections) or by using an encrypted transmission channel between the elements. Secure transmission connections prevent unauthorised use of the system.

The operation of a system in accordance with the invention is described in greater detail below with reference to Figures 4 through 6. For the purposes of this description, the system is assumed to conform to Figure 3a.

Charging can start when the user inserts his or her smart card into the card reader that is connected to the terminal. In response, the program residing in the terminal opens a window on the terminal display. This window is

called a dialog box. Figure 4 shows an example of the dialog box. Using the drop-down list of the dialog box, the user can select the type of connection required. The connections can be divided into different types, for example, by having system feature connections separate from the full-featured Internet connection, such as a permanent connection to the E-mail server, which notifies the user of new E-mail messages on a real-time basis. The latter service may be significantly cheaper (say FIM 5/day) than a full-featured Internet connection. This type of limited connection can also be created to servers other than the E-mail server, such as the workplace LAN server. The user may also use the menu to select the preferred operator or choose an encrypted and a non-encrypted connection.

The services that can be selected from the drop-down list of the dialog box can be saved in the terminal or the smart card to make it possible to open the dialog box before the terminal creates a connection to the network. Alternatively, the terminal can first automatically retrieve the most recent service list from the access server, charging server, or another network server, as soon as the user inserts the smart card into the reader. This means a slightly longer delay but then the user can always make a selection among the latest services and also receive information on the current rates. The service options offered by the dialog box can also be updated automatically during the connection, ensuring that the terminal (or the smart card) always contains a record of the services available during the last access session.

The smart card contains a record of the user profile data, which, in this example, is the user name (in ASCII format), user identifier number, the user's public and private keys, and the balance of the user's bill. The public key can be both readable and available for use. By contrast, the private key is only available for use (it cannot be read from the card). Availability for use means that the key involved can be used to create and check a digital signature, i.e. encrypt and decrypt data. The balance of the bill is the amount paid by the subscriber involved (this sum can be zeroed at any time, and so it is not the same as the final amount of the actual bill, meaning that it only serves as a reference to the user of the terminal). Moreover, the smart card can be used to save the public key of the charging server to ensure that the messages really come from the charging server.

Subscriber data, such as name, identifier, and private key can be stored in the terminal memory (on the computer hard disk or diskette) instead of on the smart card, provided that a lower level of data security is acceptable.

Figure 5 illustrates communication between the various components of the system. When the user clicks the Connect button of the dialog box, the terminal software sends the service request message Init_Service to the access server SL (Figure 5). The service request message includes at least the current IP address of the terminal (ClientAddr) and the service type (Type) selected from the dialog box menu. The access server verifies the message and transmits the start message START to the charging server WD. The start message includes the current IP address of the user (ClientAddr), the address to be notified when the user stops paying (ServerAddr), the service identifier (ServiceId), access server identifier (ServerId), and the (temporary) identifier (ConnId) which is used for identifying the various message types travelling between the servers (START and the messages OK and CANCEL, which are discussed later). Messages Init_Service and START are in this context called start messages which are used to indicate the beginning of a single access service session to the access server and to the charging server.

On the basis of the information received, the charging server WD generates a charging record (CDR, Charging Data Record) of a certain type that contains the contract data related to the access session, including the contract ID that identifies the active access session. The structure of this charging record is illustrated in a later description that applies to all charging records. The charging server sends this starting charging record (contract CDR) to the terminal (arrow A, Figure 5). The terminal returns the charging record associated with the contract to the charging server, complete with the digital signature (Figure 5, arrow B). The digital signature refers to a known encryption algorithm based on a pair of keys where encryption is carried out using the private key, allowing anyone to decrypt the message using the public key. This does not ensure that the message remains confidential, but it can be used to verify that the message has originated from the correct source. As a result, the sender cannot later deny having sent the message. When a digital signature is used, the entire message is normally not encrypted, only the digest formed from the message, which serves as a sort of check sum. From the point of view of encryption, this digest is technically very secure, and an

outsider is unable to create a message with an identical digest. The sender's private key is used to encrypt the digest and the time stamp, which together form the digital signature. There are several known optional methods of creating the signature. However, since the invention does not relate to the signing of messages, the procedure is not described in further detail here. More specific information on the subject is available in several books dealing with this field (e.g. Schneier, Applied Cryptography, ISBN 0-471-11709-9, Wiley & Sons, 1996).

The terminal can effect the signing of the contract CDR (accept the contract) automatically as described above, or the terminal can, after having received the contract CDR from the charging server, open it for view on the display in a separate contract window that once more requests the user to confirm the acceptance of the access service contract. When the user clicks the accept button in the window, the terminal transmits the signed contract CDR to the charging server.

After having received the signed contract CDR, the charging server WD verifies the signature by a known method in order to authenticate the CDR. To do so, the charging server retrieves from its subscriber database the public key for the customer involved (arrow C).

There are several way of locating the correct public key. First, the terminal can, upon receipt of the contract CDR for signing, retrieve the customer's (subscriber's) name and identifier from the smart card and add this data to the signed contract CDR which is then sent to the charging server. The charging server uses the identifier number to retrieve the correct public key from its subscriber database. Another alternative is to have the charging server check the customer identity and access right to the system before the contract CDR is formed. When the charging server receives the START message from the access server, it sends an authentication request (not shown in the figure) to the IP address contained in the START message. The terminal may insert in the reply, in addition to the customer identifier number, other customer-specific information, then adds the signature to the reply and sends the signed reply to the charging server. The advantage offered by this alternative is that the charging server knows the identity of the user before the contract is formed, making it is possible to create customer-specific tailored contracts (e.g. offering different rates for different customers). The downside is, naturally, the need for two extra messages, which slows down the setting up of the connection. A

third alternative is a system where the terminal inserts the customer identifier number into the Init_Service message before the access server forwards the identifier to the charging server in the START message. In this situation, the customer identifier number is known to both the charging server and the access server. This can be a drawback if the charging server and the access server are owned by different organisations. However, this potential drawback can be corrected as follows. The customer identifier is formed from two components. The first component identifies the origin of the customer (i.e. the customer's dedicated charging server). This component is used for routing the START message to the charging server involved. The second component is encrypted using the public key of the customer's dedicated charging server, meaning that it is not recognised by the access server. The customer identifier can also be made to look different for each instance of service, for example by attaching it to a character string of standard length that changes for each instance of service, for example as a function of time. (Thus, the customer identifier consists of the area code and signature. The area code is necessary if the ADSL connection users have contracts with different (several) charging service providers.)

The charging server saves the accepted contract CDR in its charging database (arrow D) for some time in case the customer makes a complaint about the service at a later date. After this, the charging server requests the access server to give the customer access to the network (arrow E) by sending to the access server an OK message, which includes the said identifier (ConnId) used for identifying the messages specific to that connection, as well as the contract identifier (ContractId) assigned to the service session. The access server, in turn, induces the router R1 to allow the customer to access the (Internet) network. This process is indicated by arrow F in Figure 5 and is described in more detail in connection with Figure 6.

After this, the user can access the network. This phase, during which the user uses the services provided by the network, is described in more detail later.

If the charging server does not accept the charging record (for example, if the signature is incorrect), it will send, instead of the OK message, the message CANCEL which includes the same fields as the OK message, although no contract identifier is needed at this point because the user is not given access to the network.

When the connection is terminated when the user finishes using it, a similar CANCEL message is sent (arrow G), but because disconnection is, at this point, carried out normally, the contract identifier included in the message must also be used. Thus, the CANCEL messages are identical in terms of structure but used differently in terms of function, depending on the point of time at which they are received. The access server may disconnect the user for other reasons as well, for example in the event of over-loading (if additional capacity must be reserved for vital connections, less important connections may have to be terminated), or the charging server may request the access server to close down the connection for other reasons, e.g. in the case of over-loading or in a situation, where charging records cannot be received as specified.

The start message from the terminal can also be transmitted directly to the charging server. However, when the start message is first sent from the terminal to the access server, the charging server interface can be configured identically for all service providers, making it possible for the charging server to handle billing for other service providers in addition to the access server. If the router were capable of detecting traffic initiating from a specific source address and notifying the access server thereof, no start message would be needed (as the start message would originate from the router).

Figure 6 illustrates in more detail the communication taking place between the access server and the router during the opening phase of the connection (Figure 5, arrow F). For the purposes of this example, it is assumed that the connection between the access server and router is a known Telnet connection because the SNMP protocol (Simple Network Management Protocol) cannot yet be used for updating the access lists of the router involved.

The access server SL controls the router R1 interface through which the user gains access to the Internet. The access list AL is stored in the router. As shown in Figure 6, this list can include five columns, the first column showing the IP addresses (ClientAddr) of the terminals that can use the interface involved to access the Internet, the second column showing the above-mentioned connection identifier (ConnId), the third column the contract identifier (ContractId), the fourth column the number of incoming packets, and

the fifth column the number of outgoing packets. A similar list may exist for both transmission directions of the interface.

When the access server SL has received the OK message from the charging server, it first sends the router a command that clears the access list. This command is indicated by CLEAR_AC. Next, the access server sends a command that allows all Internet protocol control messages to pass through (PERMIT_ICMP). If the charging server and/or the access server are on the Internet side of the router R1, the access server then sends the commands necessary to enable all connections to the charging server and/or access server (PERMIT_WD and/or PERMIT_SL). Finally, the access server transmits a command that permits access through the interface for a specific terminal. One such command is sent for each ongoing connection (PERMIT_ADDR1...PERMIT_ADDRN). In response to the commands, the router updates the access list. A similar update is carried out for each new connection. In other words, the entire list is first cleared and then rewritten with the new terminal added to the list.

For the access list update, the charging server sends the addresses of the terminals that are currently paying for access to the network providing the services, or at least the data on any changes relative to the previous access list.

When the user terminates the connection, the charging server sends a CANCEL message to the access server (Figure 5, arrow G). As a result, the access server updates the access list as described above so that the user involved is removed from the list during the update. This process is indicated by the arrow H in Figure 5.

If connections are set up and terminated in such a rapid succession that maintaining the list in the above manner proves too slow, the router can save several updating events and include them all in the new access list in one go.

In practice, the process described above can be employed, for example, with the CISCO router model 7000 featuring, for example, the IOS 11.2 operating system. As mentioned above, future routers will probably include features that allow more efficient updating of the access list by making changes to the items only where necessary.

When the connection has been set up, the terminal can be used to make use of the services provided by the Internet. To maintain the connection

open, the terminal generates charging records at regular intervals, sends them to the smart card for the digital signature and then sends the signed charging record to the charging server, which saves the accepted charging records in its charging database.

After gaining access to the Internet services via the router R1, the user can use his/her service browser (such as a known web browser) to locate suitable services on the Internet and to conclude additional contracts with the providers of such services. When the customer finds a suitable service, such as a Video-on-Demand service, he/she selects the service, for example by clicking the appropriate option.

When the customer has made the selection, the server of the service provider sends to the charging server WD the service identifier that identifies the film concerned as well as the identifier for the customer involved, which the server can determine, for example, on the basis of the source address of the messages received from the customer's browser program (such as the socket address of the TCP connection).

After this, the charging server WD starts the process that operates the service involved. First, the charging server retrieves from the service database the parameters corresponding to the service concerned, and sends to the terminal the contract CDR, which contains the charging parameters to be used during the service session involved as well as the contract identifier. After receiving a charging record that activates the service, the terminal program opens a window on the terminal display. This window will be referred to as the contract window below. Using the information received from the charging server, the window displays the basic data on the various parties and the service involved. Additionally, the window displays the contract identifier that identifies this particular service session. Consequently, this contract only concerns an individual service, such as the viewing of the selected film, being a service that is completely external to the access service. As a result, the system carries out charging not only for the access service but also for other services simultaneously. Such charging may depend, for example, on the contents of the service provided.

All the currently active contracts are displayed in the main window of the terminal (Figure 7a). As charging for Internet services based on the contents of the service provided is not directly concerned with the idea of the invention, no more detailed description is provided in this context. The

charging procedure is described in greater detail in the PTC patent application PCT/FI97/00685 filed by the same applicant (confidential at the time of submission of the present application).

The charging server verifies the origin of each charging record by using the public key of the customer (subscriber) involved, and saves the accepted charging records in the charging database. Each CDR to be sent from the terminal to the charging server represents a charge for access time over a certain time interval and includes a contract identifier, which is used to separate the services from one another. Because only one system user can use a specific terminal at any one time, the signatures of the charging records that are received from the source address remain unchanged during any single access session. All records of this type are accumulated specifically for each individual subscriber and contract identifier. To determine total billing for each type of service (such as access service), the system adds up the charged amounts in all the charging records related to that particular contract identifier.

From the charging database of the charging server, the CDRs are periodically transferred to the billing system BS (Figure 3), where they are processed into bills using a known method and sent to the customers. Each bill contains a list of services and charges for all of the services used by the customer during the billing period (such as one month). The bill can be delivered as a hardcopy by post, or in an electronic form to the terminal. Figure 7b shows a bill sent to the customer. The bill contains the subscriber data as well as a list of the services used during the billing period. For each individual service, the bill can specify, for example, the service type, service provider, contract identifier used for receiving the service, start time and duration of the service, and the price.

Since the operation of the billing system is known, it is not described in further detail here.

For example, the system may make use of a total of nine (0 through 8) types of charging records (charging messages) as follows:

0. Contract: This is the initial charging record (arrow A, Figure 5) that the charging server sends (unsigned) to the customer and that the terminal returns to the charging server complete with the signature, provided that the customer accepts the contract.

1. Payment: This type of charging record is sent, complete with a signature, during a service session from the customer's terminal to the charging server, which verifies it.

2. Final: This CDR is similar to type 1 except that it includes a statement indicating that it is the last CDR that the terminal is going to send during the current service session. When the user terminates the service him/herself by pressing the Quit button, the terminal first sends a CDR of type 1 and after that a CDR of type 6. In this way, the charging server can distinguish a user-initiated termination from a normal termination of the service (such as the end of the film). This type of record can also be used for one-time charging.

3. Pulse: This type of CDR is sent from the charging server to the terminal. Its purpose is to tell the terminal that it should send a new CDR if the service is to be continued. If the terminal does not send a valid CDR during a specified period of time, the charging server sends an abort message to the server of the service provider.

4. Missing sequence number: This record is sent by the charging server to the terminal (during a valid continuous billing contract) to notify that a CDR with a certain sequence number has not been received by the charging server or that the CDR received was not valid. In such a case, the terminal can send the CDR again to remedy the situation. However, this type of functionality is not necessary for either party. If the terminal does not respond to this type of CDR, the best option is to ensure that the billing system will have no right to charge for the portion of the missing CDR.

5. Modified contract: This type of CDR sent by the charging server to the customer is similar to the type 0 charging records except the contract identifier supplied in the message is not new but the same as the number of the short-term contract currently in use. This charging record is sent during a service session to indicate that the charging parameters have changed. The terminal can, for example, accept the new contract automatically, if the price has been lowered; otherwise, specific acceptance by the customer may be required.

6. Abort: This type of CDR can be sent in either direction to indicate that the contract is to be terminated. The CDR is signed by the sender.

7. Digital cash: Another way of making use of the billing system is to have a CDR (type 1 or 2) related to a certain payment include payment in

digital cash. However, the charging server does not transfer the digital cash to the billing system. Instead, the digital cash is transferred (whenever a specific and relatively small amount of digital cash has accumulated) directly to the server of a bank or a network server of some other organisation, which then debits the customer's account directly. Digital cash can be used along with the centralised billing system BS in the same way as in electronic commerce, or as an alternative to centralised billing.

8. Synchronisation of charging: This record is sent by the charging server to the terminal (during a valid continuous charging contract) to indicate that the payment CDRs do not cover the per-minute rates of the continuous contract (when, for example, the terminal clock is running too slowly). The synchronisation CDR indicates how much the customer should pay to maintain the contract operative.

Figure 5 illustrates the charging procedure for a single service. The category of each message is indicated above the arrow symbolising the message. The figure illustrates a situation where the charging server detects once during the service that a certain charging record is missing.

Depending on the number of processes being executed simultaneously on the terminal, the interval between two consecutive type 1 CDRs can vary. If the load that the terminal is subjected to increases very much and CDR generation is delayed relative to rated performance, the charge included in the CDR is, correspondingly, greater.

In practice, continuous charging involves two time-related problems. First, one or more payment CDRs may be lost because of a failure or an error. Second, the terminal clock may run more slowly than the charging server clock. To eliminate these problems two threshold values (A and B) are defined. The first threshold value (A) is the maximum outstanding debt that the user can owe to the charging server as a result of use that remains unpaid. The second threshold (B) is the maximum value of outstanding debt following payment. Both limit values are linked to independent timer values (T_A and T_B).

Figures 7c and 7d illustrate a solution to the said problems. The time axis t represents the time of the charging server and the time axis t1 the time of the terminal. In the figures, the time is expressed in seconds. The vertical axis at the top of the figure shows the user debt to the charging server while the lower section shows the charging records sent by the charging server and the terminal. For the purposes of this example, network delay is assumed to

be negligible. In Figure 7c, the clocks run at the same speed, but in Figure 7d the terminal clock is slower than that of the charging server. At the moment t1=0 the terminal sends the signed contract (CDR-0) to the charging server. The charging server receives the contract at the moment t=0. The user debt D(t) begins to increase as of this moment. As no payments are received, the debt increases linearly as a function of time. The rate of increase of the debt (money units per time unit) is defined in the contract. When the charging server receives a payment CDR (CDR-1), the debt is reduced by the amount stated in the CDR involved.

After receiving the contract, the charging server calculates the balance of the debt periodically (for example, once a second). If D(t) > A, the charging server sends a type 4 CDR to the terminal. If the charging server does not receive the outstanding payment within the time T_A, it terminates the contract. Figure 7c shows a situation where a payment CDR (CDR-1) sent at the moment t1=120 fails to reach the charging server. As a result, the debt incurred exceeds the threshold value A before the following regular payment is made. Then, the charging server sends a type 4 CDR to the terminal and the terminal re-sends the payment CDR in response. It is also possible to define a maximum period of time that the charging server can operate without receiving a payment CDR. If this time limit is exceeded, the charging server sends a type 4 CDR.

The charging server checks the amount of debt following each regular payment, if not more frequently. If the terminal clock runs at a slower speed than the charging server clock, as shown in Figure 7d, the balance of the outstanding debt after the payment increases payment by payment. When the amount of outstanding debt after the payment exceeds the threshold value B, the charging server sends, to the terminal, a type 8 CDR (synchronisation), which contains information concerning the amount of the desired payment. In response, the terminal transmits a signed synchronisation CDR. If the charging server does not receive the outstanding payment within the time T_B, it terminates the contract.

All charging information required by the system is transferred in the sequential fields of protocol messages (charging records). The fields contained in the charging records are shown in Figure 8:

TYPE: Indicates the type of the CDR, i.e. which of the eight above-mentioned charging records is involved.

LENGTH: This field indicates the total length of the CDR in bytes, including the type and length fields.

CONTRACT NUMBER: This field includes an integer given by the charging server. The number is identical for all the CDRs that relate to the same charging session.

SEQUENCE NUMBER: An integer that indicates the order of generation of the CDRs during one charging session. The terminal assigns the number 0 to the first contract CDR (type 0) it returns, after which the number is increased in increments of one. This field is not defined for CDR types 3, 5, 6 and 7, and in type 4 it indicates the sequence number of a missing CDR.

SERVICE IDENTIFIER: The contents of this field indicate the service for which the customer is being charged. The value of the parameter in this field is based on a contract between the billing service provider and the (multimedia) service provider.

SERVICE TYPE: The parameter in this field is used for a rough classification of the services for statistical purposes, such as web sites, Video-on-Demand, file transfers, etc.

STARTING TIME: The parameter in this field shows the current time for CDR types 0 and 5 and also 3, 4 and 6, and the start time for the charging period for types 1 and 2.

ENDING TIME: The parameter in this field defines the ending of the charging session for CDR types 1 and 2. With CDRs of types 0 and 5, the field parameter specifies how often the charging server expects to receive a payment CDR. This parameter is not defined for other types of CDRs.

IDENTIFIERS: The parameter in this field indicates the customer, charging server and server identifiers. The identifiers can be integers or network addresses, but they must be unique within the billing system.

METHOD OF PAYMENT: The parameter in this field is defined for CDR types 0, 5, 1 and 2. For example, the methods of payment may be classified as follows: *free*, *one-time charge* (one CDR), *periodic* or *externally triggered*, i.e. another process in the terminal may trigger it. For example, a terminal video player program can trigger CDR generation once a minute, if an acceptable video signal has been received during the preceding minute. A system in which the charging server triggers CDR generation using the parameter in the method of payment field is described later.

AMOUNT OF MONEY: This field indicates the debt incurred by the customer (either for the entire session or for a period of time between two CDRs).

TRAFFIC DATA: This field contains information transmitted from an external application on the terminal to the terminal and forwarded to the network.

SIGNATURE: This field contains the customer's digital signature, which is used for the authentication of the CDR.

Appendix 1 provides a more detailed description of the structure of the CDR using the Abstract Syntax Notation 1 (ASN.1), which is a common description language for data structures used in the telecommunications field. In addition, the appendix also explains the structure of the Init_Service, START, OK and CANCEL messages.

Charging records and the said messages can be sent, for example, in the data field of IP packets, which may contain one or more charging records.

Charging operates correctly when the network access and payments are in synchronisation with one another, i.e. when the paying customers have access to the network providing the services and the non-paying customers do not. For example, a fault may lead to a situation where the router denies paying customers access to the network providing the services or allows access for non-paying customers (who do not send payment CDRs). To correct such a situation, the access server polls the router and the charging server. From the router, the access server obtains the access list and from the charging server the IP addresses of the customers who are paying for access to the network at that particular moment. If the address of a paying customer is not included in the access list, the access server adds the address to the list. If an address included in the access list is not included in the list of paying customers in the charging server, the access server removes the address from the list. The system can be configured to allow the service provider to set the desired polling interval.

Figure 9a illustrates the operation of the terminal (CT) by means of a functional block diagram. As far as the present invention is concerned, the most important part of the device consists of the CDR generator CG that generates the charging records. Connected to the CDR generator is the security library SLI, whose memory contains the customer's private encryption

key and which executes the signing of the charging records. The CDR generator creates the CDRs and transmits them to the security library where they are signed using the customer's private encryption key. The security library returns the signed CDRs to the CDR generator, which forwards them to the charging server WD.

If the application or the environment is such that encrypted messages must be exchanged between the terminal and the charging server, the security library executes the encryption, signing and signature verification.

The security library can be a hardware-based or a software-based solution. However, the hardware-based solution offers better security. Thus, the security library, or part of it, can be construed as described above using a smart card that contains, for example, the private encryption key of the customer.

Additionally, the terminal contains elements for receiving the service. These can include, for example, a service player VP, which can be a video player reproducing the video signal received from the network and may also give the CDR generator commands to generate charging records. The service browser SB, the service player VP, and the CDR generator are connected to the network via the terminal's communications library CL. The CL puts together the protocol stack according to which the terminal operates. This protocol stack may, for example, consist of a TCP/IP stack, such as Microsoft's Winsock.

The start-up logic unit SUL of the terminal initiates the sending of the start message to the access server when the user inserts the smart card in the reader.

The terminal can also incorporate a charge counter BC that the customer can use to check the accuracy of the bill sent by the service provider. In addition, the terminal can include various components for monitoring the quality of service (QoS) of the information flow received. For example, a video player can give the source the command to stop transmitting information when the quality of service falls below a certain level.

Figure 9b shows the functional block diagram of the CDR generator in greater detail. The contract logic unit CLU1 handles the generation of charging records based on the information stored in the configuration database CDB. It contains the logic that transfers the received contract information to the graphical user interface GUI and generates the type of

charging records described above. This logic includes timing components TM that define the time elapsed between two consecutive CDRs. The contract logic unit CLU1 is connected to the communications library and the network via an external control interface ECI, and to the service player via an internal control interface ICI. The external control interface carries out the conversion between the internal and external CDR formats. The internal control interface handles message transfer between the service player and the contract logic unit and performs the necessary conversions between the message format used by the service player and the internal message format of the equipment. The connection between the internal control interface and the service player (interface A3) can, for example, be realised using a communications library (TCP socket). The configuration database CDB is used for saving the settings made by the user (user preferences), and it can also be used for storing information on various services (such as films) displayed to the customer in response to the service identification received. This database can, for example, be created with Microsoft Access or Borland Paradox. The configuration database is controlled via the management unit MM. The management unit, the configuration database and the contract logic unit are all connected to the graphical user interface (GUI) of the device, which can, for example, be implemented using Java applets or the Microsoft Visual Basic programming tool. Part of the configuration database can be located in the network.

If the service player is designed, for example, for Video-on-Demand, it can, for example, be implemented using a personal computer and a program designed for Video-on-Demand services. One such program is StreamWorks offered by Xing Technology Inc., USA.

The management unit and the contract logic unit are linked to the security library via the A1 interface. The security library and the A1 interface can be implemented, for example, using the SETCOS 3.1 smart card (and smart card reader) from Setec Oy or some equivalent product based on the international smart card standards. (The international standardisation organisation ISO has defined a series of smart card specifications as follows: ISO 7816-1 (physical dimensions), ISO 7816-2 (location of contacts), ISO 7816-3 (transmission protocols) and ISO 7816-4 (command and file structures).)

A user may have several different smart cards, each of which opens a certain type of connection. One card can, for example, be used for setting up

a fully featured Internet connection while another card (whose subscriber is the employer) may only be used for accessing the LAN at the workplace.

Figure 10 illustrates the structure of the charging server WD by means of a general block diagram. The core of the equipment consists of the contract logic unit CLU2 that has access to the service database SED, the subscriber database SUD, and the charging database BD. The service database contains information about the services offered by the various service providers and the parameters for charging for the use of the services. The charging server can also change the charging parameters independently, for example according to the time of the day. The subscriber database contains the customer data for the operator that manages the charging server (including the public key of each customer). The charging records received from the terminals are saved in the charging database. An encryption block CM is associated with the contract logic unit to verify the charging record signatures. This block corresponds to the SL block of the terminal. The contract logic unit receives from the terminals charging records signed by the terminals and forwards them to the encryption block for verification. The contract logic unit saves the accepted charging records in the charging database. The contract logic unit is connected to the network through the communications library CL that forms the protocol stack defining the connection to be set up.

In practice, the contract logic units complete with the functions described above can, for example, be implemented using tools based on the international System Description Language (SDL) standard, such as the SDT tool from Telelogic AB.

The databases of the charging server can reside in the memory MS described above (Figure 3) and are located in connection with the charging server. In addition, the charging records can be saved in a separate mass memory MS1 (Figure 3) which is located between the charging server and the billing system in the network and which is organised in such a way that the billing system can easily handle the information stored in it. By using this type of separate database, it is possible to let the service providers use the database for various queries in order to develop their services. For example, the service provider or customer can request information on charges generated by a certain service in the middle of a billing period (using E-mail or similar).

Figure 11 illustrates the structure of the access server SL by means of a functional block diagram. For external connections, the server features an interface unit IU, which comprises the router interface unit RIU, the charging server interface unit WIU, and the terminal interface unit TIU. The TIU receives the aforementioned starting message Init_Service from the terminal and initiates the billing session for the customer involved. The router interface unit monitors the router access list while the charging server interface unit handles communications with the charging server. The connection logic CLO is a simple state machine that links the various interface units. The connection logic also maintains a list of all open connections and two queues, one of which contains the connections to be terminated and the other the connections which are to be set up.

The router control unit RCU, which includes the router command set, controls the router by handling the maintenance of the aforementioned access list.

The synchronisation unit SU carries out synchronisation of the said payments and access rights by comparing, at certain intervals, the router's list of open connections with the addresses of paying customers obtained from the charging server. Any conflicts are corrected, ensuring that no error in charging persists longer than the said interval.

The router connection control unit RCC monitors the connection between the access service and the router. As it is assumed for the purposes of the example that the connection between the router and the access server is a Telnet connection, the router breaks the connection if it remains inactive for too long a time. The task of the router control unit is to activate the connection if the router happens to break it, for example, for the above reason or because of other interferences in the connection.

The volume monitoring unit VCU and the charging database BD2 used by it are included in the access server, at least if charging is to be based on the volume of transferred data. In such a case, the control unit uses the router access list to check the packet counts through the router interface unit and saves the data in the charging database BD2, ensuring that the number of packets and the IP addresses used by the terminal for the connection are stored for each individual contract identifier. When the services are billed for, the data in the access server charging database are combined with the data in

the charging server charging database according to contract identifier. This makes it possible to take account of the volume of transferred data in the bill.

The embodiment described above does not, as such, provide the addition of the subscriber signature to the packet count data, meaning that the user would have to take the packet counts determined by the system on trust. However, in all other situations the terminal can verify that charging is carried out correctly. To solve this problem, a two-phase procedure is adopted. First, the access server notifies the terminal when the volume to be charged has been increased by a certain value (for example by 50 Mb). In this way, the terminal can monitor the volume count performed by the access server and compare it against its own records. Second, the access server sends each volume-related CDR to the charging server, which forwards it to the terminal for a signature. The procedure is similar to the signing of the contract described above; it offers the terminal user an opportunity to monitor charging and makes it difficult to repudiate bills. This method is explained below in more detail with reference to Figure 12, which illustrates the communication between different elements.

First, as described above, the system creates a separate "volume agreement" in the form of a contract that is triggered externally (arrows 121 to 124). The access server reads the desired packet counts from the router and saves the data in the charging database BD2. When the packet count reaches a predefined limit, the access server sends a signed CDR of type 3 (pulse) to the charging server (arrow 126). However, prior to this, the access server sends to the terminal traffic data port a message VM, which contains information on the volume of transferred data (indicated by the term "traffic data"). Thus, the volume information will be included in the next CDR to be signed, and the user, or at least the terminal, will have the opportunity to verify the volume before the CDR is signed.

When receiving a type 3 CDR from the access server, the charging server identifies the contract as an externally triggered contract and forwards the CDR involved to the terminal (arrow 127). If the user or the terminal accepts the volume count, the terminal generates a payment CDR, inserts the received data volume information in the traffic data field of this payment CDR, and sends the payment CDR to the charging server (arrow 128). The charging server forwards the CDR, or the data contained in it, to the access server (arrow 129) that verifies at least the data contained in the traffic data field.

Depending on the outcome of such verification, the access server either terminates the service or allows it to continue. In this case, the service provided probably consists of a combined service that includes both a time-based and a volume-based contract.

From the point of view of the terminal, the volume-based charging described above takes place as follows. The charging server sends a new contract (arrow 122) whose method of payment parameter contains a value indicating an externally triggered payment. When the payment is required, the terminal receives a type 3 CDR that indicates the amount of the payment required. The terminal either automatically accepts the payment or the data are shown on the terminal display to allow the user to decide whether to accept the payment transaction. If the payment is accepted, the terminal changes the CDR type to 1 (payment CDR), signs the CDR, and sends it to the charging server (arrow 128).

A payment transaction can also be triggered by some other external object, such as the charging server sending the terminal a command indicating that payment should be effected. This type of command is transmitted to the socket address that corresponds to the traffic data. In addition to the actual command ("effect payment"), the command message also includes the contract identifier information. After this, the terminal makes the payment. In this case, the command only states that a payment is required. The actual amount of payment is defined by the contract.

Volume-based charging, as described above, can be carried out in such a way that the terminal or the user is constantly aware of the size of the bill being incurred. As every payment must be accepted, repudiation of charges is extremely difficult. Messages are only sent when payments are required, so if there is no traffic to or from the terminal, no blank or superfluous charging messages are generated either. Because this feature is implemented on the application level, volume-based charging is not restricted to any specific technology, and there can be several "chargers" between the service provider and the terminal simultaneously charging for services on a volume basis.

Although the above example is based on the ADSL environment it is obvious that the method according to the invention offers the same advantages in any connectionless network providing access services where it is necessary to identify each individual user of a certain network address, or where the user is not necessarily the service subscriber who pays for the

service. The terminal can also be connected to a network providing services through a wireless connection. Future types of connection may vary considerably.

In the foregoing, reference was made to situations where the user network address (IP address) may change from one service session to another while remaining unchanged during any single service session. However, the method according to the invention can also be applied in situations where subscribers move from one location to another. To accomplish this, use can be made of the Mobile IP protocol, which is a version of the existing IP that supports terminal mobility. (The principle of the Mobile IP is explained, for example, in the article *Supporting Mobility with Wireless ATM*, by Upkar Varshney, published in Internet Watch, January 1997.)

Mobile IP is based on a system where each mobile host or mobile node has an assigned agent ("home agent") that forwards the packets to the current location of the mobile host. When the mobile host moves from one subnetwork to another, it registers with the agent ("foreign agent") serving the subnetwork involved. The foreign agent carries out a number of checks with the home agent of the mobile host, registers the mobile host and sends the registration information to it. The packets addressed to the mobile host are transmitted to the original location of the mobile host (the home agent) from where they are forwarded to the current foreign agent, which, in turn, forwards them to the mobile host.

When the principle described above is applied to a system based on the invention, each user can have a dedicated (home) charging server that manages the user's public keys and serves as the home agent. The access servers (i.e. the foreign agents) serving the various subnetworks indicate to the charging server when to start charging. The charging server involved retrieves the public keys from the user's home charging server and takes over the charging function. What is essential is that the subscriber's public key can be securely transferred to a charging server close to the subscriber to make it possible for the charging server to verify the charging records. (If such transfer cannot be securely carried out, a third party may be able to modify the key during transfer and thus generate expenses that will be included in the bill of the original subscriber). For example, the subscriber's public key can be transferred to a database that is close and accessible to the charging server. The closest charging server can handle charging using the identifier of the

subscriber's dedicated charging server. The CDRs accumulated during the session will be transmitted to the subscriber's dedicated charging server when the service session is terminated.

Communication between the various components in a system using the mobile IP is illustrated in Figure 13. In the figure, the home and foreign agents are shown as physically separate elements, but as previously indicated, the access server can also serve as the foreign agent while the home charging server can serve as the home agent. In accordance with the mobile IP, the foreign agent FA continuously transmits, to its own subnetwork, broadcast messages known as "agent advertisements" and indicated in the diagram by the letters AA. When the terminal connects to the said subnetwork, it will receive these messages and deduce from them whether it is connected to its own home network or some other network. If the terminal detects that it is connected to its home network, it will operate without any mobility services. Otherwise, the terminal will be given a care-of address for the foreign network. This address is the address of the point in the network to which the terminal is temporarily connected. At the same time, this address constitutes the termination point of the tunnel leading to the terminal involved. Typically, the terminal receives the address from the previously mentioned broadcast messages that the foreign agent keeps sending. In response, the terminal sends the registration request RR to its home agent via the foreign agent FA. The request includes, among other things, the care-of address just assigned to the terminal. In response to the request, the home agent updates, in its database, the location data for the terminal involved and sends the registration reply R_Reply to the terminal through the foreign agent. The reply message contains all the necessary information on how (on what terms) the home agent has accepted the registration request. All the messages between the terminal, foreign agent and home agent described above are standard mobile IP messages.

After this, the foreign agent FA sends the above-mentioned start message, i.e. the charging service request Init_Service to the access server SL. This message is equivalent to the service request message shown in Figure 5, indicating the beginning of a single service session. The message includes, among other things, the care-of address of the terminal involved. As of this point, the system operates as shown in Figure 5, except for termination of charging and the acknowledgement message ACK, which will be discussed

later. Next, the access server checks the message received and forwards the start message START to the charging server WD. This is followed by contract negotiations between the charging server and the terminal, the usual outcome of which is that the user is given access to the network.

Termination of charging differs from that of fixed terminals shown in Figure 5 in that the termination can, in a mobile IP environment, be effected either by the foreign agent or the charging server, depending on which of the elements first detects the change. If the foreign agent detects that that the user has exited the network, it will send the end message CANCEL(1) to the access server. The access server forwards the said message to the charging server and closes down the router for the connection involved. The foreign agent will automatically detect the user exit because the mobile IP requires regular messages from the terminal to indicate its continued presence in the subnetwork. These "alive" messages are intended only for the home agent, which does not forward them. However, if it is the charging server that detects the user exit first, it will send the access server the end message CANCEL(2), which removes the connection from the router. In all other respects, the termination of the connection includes the same options as described above.

In the case of mobile IP, the user or the terminal does not, then, send the start message (as shown in Figure 5); instead, the operation of the foreign agent is modified to allow it to initiate charging when the terminal connected to the subnetwork that it serves registers with its dedicated home agent through the foreign agent.

In addition, the foreign agent maintains a special charging initiation timer that starts when the service request message is transmitted to the access server. If no ACK message is received before the timer expires, the foreign agent attempts to re-start charging by sending a new service request to the access server. This is a process that the foreign agent performs for all the terminals in its area with no on-going charging.

By using the procedure described above, the access service provider can reliably restrict the users to those who can be charged access to the network although the mobile IP, as such, does not offer such a feature.

It should be pointed out that a foreign agent is not absolutely necessary for a mobile IP network. If no foreign agent is used, the network will still include a DHCP server or other mechanism for assignment of temporary addresses. If, in such a situation, the terminal is to use mobility services, it

must register with its home agent. Then, the DHCP server or home agent may serve as the access server, depending on the network configuration.

The foregoing description relates to the access service for mobile IP connections. If the routing protocol is IPv6, which has no special foreign agent, the access service must be initiated somewhat differently.

When an IPv6 terminal is connected to a new network, the default procedure is that the terminal waits for an advertisement message from the router. This message may give the terminal permission to generate its own address or obligate the terminal to use the DCHP server for a temporary address. After receiving the said temporary address, the terminal sends binding updates that are used to update the data on network routers relating to the (fixed) home address of the terminal and the associated temporary address. These binding updates are transmitted to all the nodes that the terminal communicates with, in particular to the dedicated home agent of the terminal. Using these binding updates, the nodes update their routing data to be able to forward the packets intended for the terminal involved directly to its temporary address.

Figure 14 provides a simplified description of the message exchange between the various components when the routing protocol is IPv6. In this case, the routers may require that the new users (terminals) connecting to the network register with the local DHCP server DHCP_S. The terminal sends the DHCP server the registration request (REQUEST) in response to the advertisement message it received. After assigning a temporary address (message ACK) to the terminal, the DHCP server initiates charging by sending the start message Init_Service to the access server SL. From the point of view of the charging and access servers, the DHCP server thus assumes the same role as the foreign agent in a mobile IP network. More precisely, by sending the said start message, it informs the access server of the new terminals that are being connected to the network. In all other respects, the protocol is similar to the above-described mobile IP case (in which the network includes a foreign agent).

In this case, the default configuration for the gateway router R1 must allow all terminals connecting to the network to access the access and charging servers.

When a terminal moves from one subnetwork to another (i.e. from one access server to another), it is possible to negotiate a new contract,

renegotiate the existing contract or renew the same contract depending on how the conditions will change as a result of handover. For example, if the operator also changes at the same time, a new contract can always be negotiated. If the operator remains unchanged but the quality of service provided by the new network is markedly different from that provided by the previous network, the existing contract can be revised by renegotiating the terms. The party making the decision on the handover event should also decide whether the existing contract is terminated or renewed. At any rate, the user has a right to know which network he or she has accessed and on what terms the service is provided.

The network environments illustrated in Figures 13 and 14 are similar to the examples given in Figures 3a through 3d, except that the LAN switch is replaced by a wireless (or wired) access network, ATU-C is replaced by a joint access point, such as an intelligent hub or similar, and ATU-R is replaced by the terminal interface (card). In addition, the DHCP server is replaced by a foreign agent, if the network involved is a mobile IP network. Figure 15 illustrates the latter network environment using the example given in Figure 3a. Here, the foreign agent is shown as a separate unit, although it can be incorporated in the access server. As indicated in the figure, the local charging server of the access point is typically separate from the dedicated charging server of the user accessing the network through the said access point, while the said dedicated charging server could be connected to the Internet or the telephone network.

Although the invention has been described above with reference to the examples shown in the attached drawings, it is obvious that the invention is not limited to these examples but can be varied within the limits set by attached patent claims. A brief description of conceivable variations is provided below.

For example, it is possible that the terminal need not send the actual charge but some other (charge-related) messages to the charging server, which the charging server can then use for generating the charging records by itself. For example, the terminal can send so-called keep-alive messages for the duration of the service, after which the charging server may only generate one charging record, where the duration of the service is equal to the time that has elapsed from the last keep-alive message to the moment when the contract was accepted. Similarly, it is possible, particularly in

systems that support terminal mobility, that some other network element or entity, such as the access server or foreign agent assumes the role of the terminal as the generator of the charging record(s). Such an element or entity must enjoy the user's full confidence. Assuming the role of the terminal can, for example, be effected by having the terminal pay a certain lump sum to the said element or entity which then maintains the connection in accordance with the payment received and possibly requests additional payments from the terminal. If the entity representing the terminal generates the charging record using its own signature, the charging server must know the identity of the party that the said entity represents from time to time. Charging records can also be generated by the interface elements that provide access for the terminals to the network providing the services. For example, this type of situation may arise when a known General Packet Radio Service (GPRS) terminal has access to an IP network through a GPRS network via the network element between the said networks (which in this case is the Gateway GPRS Support Node).

Instead of the digital signature, it is also possible to employ some other known method for ensuring, for billing purposes, that the charging records have not been tampered with in transit and that the sender data in the messages are correct. Essential to the invention is that the charging records are verifiable. For example, between the network element generating the charging messages and the network element checking the same there could be a secure transmission channel, or the charging messages could include electronic cash. If electronic cash is used, no verification of the subscriber is carried out; instead, verification will be limited to checking the structural integrity of the charging messages and cashing in of the electronic payment received from the user, which will typically be carried out by means of a special server, such as a bank's server.

The element linking the network providing the services and the access network could also consist of any suitable device that is capable of passing traffic selectively, such as a packet filter or a firewall. In addition, some other message sent for another purpose can also serve as the start message indicating the beginning of a new service session.

```
-- The CDR structure
-- ================
-- In the initial version the encoding is byte-oriented
-- without tag and length fields. ENUMERATED is encoded
-- as one octet if nothing else is specified, INTEGER
-- is encoded as an octet string (length 2, 4 or 8 depending
-- on the maximum size) in MSB first format.

CDR_cdrType ::= ENUMERATED {
        contract    (0), -- initial CDR, WD -> Client
        payment     (1), -- normal payment CDR
        final       (2), -- as above, client stops
        pulse       (3), -- indication of new payment
        missing_seq (4), -- CDR with seq.num. lost
        mod_contract (5), -- contr. renegotiation
        abort       (6), -- end connection, no money inc.
        E_cash      (7)  -- e_cash carrier CDR, type B
}
-- Types 0..6 are overloaded onto a CDRtypeA, type 7 uses
-- a CDRtypeB

CDR_network ::= ENUMERATED {
        unknown         (0),
        TCP/IP          (1),
        ISDN            (2)}

CDR_serviceTypeType ::= ENUMERATED {
        unknown         (0),
        ...
}
```

```
CDR_timeType ::=
   hundrethOfSec   OCTET STRING (SIZE(1)),
   seconds         OCTET STRING (SIZE(1)),
   minutes         OCTET STRING (SIZE(1)),
   hours           OCTET STRING (SIZE(1)),
   days            OCTET STRING (SIZE(1)),
   year_lo         OCTET STRING (SIZE(1)),
   year_hi         OCTET STRING (SIZE(1))}

CDR_identifierType ::= SEQUENCE {
   type      ENUMERATED {system_assigned(0),
E164_addr(1), ...}
   data      OCTET STRING (SIZE (16))
}

CDR_paymentMethodType ::= ENUMERATED {
      free    (0), -- no charge
      one_time (1), -- agreement valid for one payment
      periodic (2), -- time-based
      wd_req  (3), -- payment triggered by a WD msg
      ext_trig (4)  -- paym. trigg. by an extern. client. appl.
}

CDR_currencyType ::= ENUMERATED {
   majorType   ENUMERATED {bill(0), E_cash(1)},
   currency    ENUMERATED {FiM (0), USD(1), ...}
}
-- encoded in one octet so that majorType occupies
   the most significant bit and currency bits 0-6
```

```
CDR_moneyAmountType ::= SEQUENCE {
   currency   CDR_currencyType,
   value      INTEGER(0..MAX_WORD)
-- in case E_cash is used, the value defines the
-- sequence number of the E_cash carrier CDR

CDR_signatureType ::= SEQUENCE {
  present   ENUMERATED {absent(0), present(1)},
  type      ENUMERATED {RSA-with-MD5(0), DES-with-MD5(1)},
  signature OCTET STRING SIZE (64)
}

CDRformatA ::= SEQUENCE {
  type        CDR_cdrType,
  length      INTEGER (0..MAX_S_WORD),
  contractNr  INTEGER (0..MAX_D_WORD),
  sequenceNr  INTEGER (0..MAX_WORD),
  serviceId   INTEGER (0..MAX_D_WORD),
  serviceType CDR_serviceTypeType,
  startTime   CDR_timeType,
  endTime     CDR_timeType,
  clientId    CDR_identifierType,
  watchdogId  CDR_identifierType,
  serverId    CDR_identifierType,
  payMethod   CDR_paymentMethodType,
  moneyAm     CDR_moneyAmountType,
  trafficData OCTET STRING (SIZE(8))
  signature   CDR_signatureType
}
```

```
CDRformatB ::= SEQUENCE {
  type        CDR_cdrType,
  length      INTEGER (0..MAX_S_WORD),
  contractNr  INTEGER (0..MAX_WORD),
  sequenceNr  INTEGER (0..MAX_WORD),
  e_cash      OCTET_STRING(SIZE(0..200))
}

Start ::= SEQUENCE {
      MessageType    OCTET_STRING(SIZE(1)) DEFAULT(1)
      MessageLen     INTEGER(0..MAX_LEN),
      ClientAddr NWAddr,
      ServerAddr     NWAddr,
      ServerId       CDR_identifierType,
      ServiceId  INTEGER (0..MAX_D_WORD),
      ConnId     INTEGER (0..MAX_WORD)
}

OK ::= SEQUENCE {
      MessageType    OCTET_STRING(SIZE(1)) DEFAULT(2)
      MessageLen     INTEGER(0..MAX_LEN),
      ContractId INTEGER (0..MAX_D_WORD),
      ConnId     INTEGER (0..MAX_WORD)
}

Cancel ::= SEQUENCE {
      MessageType    OCTET_STRING(SIZE(1)) DEFAULT(3)
      MessageLen     INTEGER(0..MAX_LEN),
      ContractId INTEGER (0..MAX_D_WORD),
      ConnId     INTEGER (0..MAX_WORD)
}
```

Patent claims

1. A method for implementing an access service in a telecommunications network including an access network (N1), a network providing services (N2), and user-operated terminals (TE1...TE3, PC) connected to the access network, wherein

- the access service is provided by connecting, through interface elements linking the access network with the network providing the services, the user terminal to the network providing the services,

- at least one charging record is generated in response to the access service, said record being forwarded to the billing means (BS) for charging a subscriber for the access service,

characterized in that, within the data transmission network

- the beginning of a single service session is indicated by generating a start message for charging purposes when the user contacts the access network by means of a terminal,

- verifiable charging messages related to said access service session are generated,

- the generated charging messages are verified, and

- the terminal ~~is given~~ access to the network providing the services, ~~provided that~~ said messages are generated in an acceptable manner.

2. A method according to patent claim 1, characterized in that the charging messages are generated by the terminal.

3. A method according to patent claim 2, characterized in that the verifiability of the charging messages is ensured by the inclusion of a subscriber-specific digital signature.

4. A method according to patent claim 2, characterized in that the verifiability of the charging messages is ensured by means of a secure data transmission channel.

5. A method according to patent claim 2, characterized in that the terminal is given access to the network providing the services, provided that said charging messages are received at a predefined rate and that the verifications associated with the messages are determined to be correct.

6. A method according to patent claim 2, characterized in that the terminal also transmits data on the subscriber associated with the

current user of the terminal, whereby said data is used to check the verifications and to allocate the charging messages received from the terminal to the bill of the subscriber involved.

7. A method according to patent claim 2, characterized in that at least one dedicated charging server (WD) is used in the network in such a way that each terminal has a charging server specifically assigned to it, the charging server receiving the charging messages generated by the terminals.

8. A method according to patent claim 2, characterized in that once the terminal gains access to the network providing the services, the terminal generates, at specific intervals, charging records complete with subscriber-specific verifications, each such record representing the charging for a certain period of access time.

9. A method according to patent claim 7, characterized in that the start message contains the current address of the terminal to be forwarded to the charging server.

10. A method according to patent claim 9, characterized in that the start message is forwarded from the terminal to the charging server via a special access server (SL).

11. A method according to patent claim 10, characterized in that in response to the start message received, the charging server sends to the terminal a contract message indicating that the user must negotiate a contract concerning the access service.

12. A method according to patent claim 11, characterized in that the terminal returns the contract message complete with subscriber-specific verification, the charging server checks the verification and the charging record and, when finding these correct, initiates the process to connect the terminal through the interface elements (R1) to the network providing the services.

13. A method according to patent claim 6, characterized in that the identify of the subscriber associated with the user using the terminal is indicated in the start message.

14. A method according to patent claim 12, characterized in that the identity of the subscriber associated with the user using the terminal is forwarded to the charging server in the contract message.

15. A method according to patent claim 9, characterized in that, in response to the start message received, the charging server requests from the terminal data that define the identity of the subscriber.

16. A method according to patent claim 12, characterized in that the charging server initiates the process by giving a connect command to the access server (SL), which is used for controlling the interface elements (R1).

17. A method according to patent claim 16, characterized in that the interface elements comprise a router, and the access server maintains a router access list containing the addresses of the terminals with access, through the router, to the network providing the services.

18. A method according to patent claim 2, characterized in that, in addition to the access service, charging records are generated by the terminal specifically for each service used in the network providing the services.

19. A method according to patent claim 7, characterized in that charging information contained in the charging messages is sent from the charging server to a separate billing system (BS) for the generation of subscriber-specific bills.

20. A method according to patent claim 19, characterized in that the charging information is transmitted to the billing system used in the public telephone network.

21. A method according to patent claim 17, characterized in that the access server, at predefined intervals, compares the list of paying terminals on the charging server with the list of paying terminals on the router and connects terminals to the network providing the services or disconnects the same if the router list differs from the charging server list.

22. A method according to patent claim 1, characterized in that at least part of the connection between the interface elements and the terminal is established in the form of a wired xDSL connection.

23. A method according to patent claim 1, characterized in that the connection between the terminal and the access network is wireless.

24. A method according to patent claim 1 in a network that uses mobile IP for the routing protocol, whereby the terminal, when connecting the access network, is assigned a temporary address, which it registers by

sending its home agent a registration request via a foreign agent in the access network, c h a r a c t e r i z e d in that said start message is generated by the access network foreign agent in response to registration.

25. A method according to patent claim 16 in a network that uses mobile IP for the routing protocol, whereby the terminal, when connecting to the access network, is assigned a temporary address, which it registers by sending its home agent a registration request via a foreign agent in the access network, c h a r a c t e r i z e d in that

said start message is generated by the access network foreign agent in response to registration and that the charging servers serve as the mobile IP home agents and the access servers as the foreign agents serving the various subnetworks, said foreign agents being used for indicating to the dedicated charging server of each terminal the subnetwork in which the terminal involved is located at any given time.

26. A method according to patent claim 1 in a network that uses a routing protocol that supports terminal mobility, c h a r a c t e r i z e d in that the network includes at least one server that allocates temporary addresses (DHCP_S) such that

- when a terminal connects to the access network, it registers itself with the server allocating addresses, and

- said start message is generated by the server that allocates addresses in response to registration.

27. A method according to patent claim 8, c h a r a c t e r i z e d in that when the terminal gains access to the network providing the services, the terminal receives a payment request message every time that the volume of data transferred during the service session exceeds a predefined limit.

28. A method according to patent claim 27, c h a r a c t e r i z e d in that the terminal receives information on the volume of data corresponding to the payment request message or on the amount of payment corresponding to the payment request message.

29. A method according to patent claim 7, c h a r a c t e r i z e d in that the charging server, upon reception of the charging message from the terminal indicating payment, determines the current debt incurred by the user, and if the debt, following the said payment, still exceeds a specific pre-defined limit (B), the charging server sends the terminal a message indicating that additional payment by the terminal is required.

30. A method according to patent claim 16, c h a r a c t e r i z e d in that the termination of the connection between the terminal and the network providing the services is initiated by the charging server in response to pre-defined events, including situations (i) where the charging server does not receive the charging messages in an acceptable manner and (ii) where the charging server receives a special end message from the terminal or charging server.

31. A method according to patent claim 30, c h a r a c t e r i z e d in that the access server is additionally authorised to independently terminate the connection between the terminal and the network providing the services in response to a set of pre-defined events.

32. A system for implementing access service in a telecommunications network comprising an access network (N1), a network providing services (N2) and user-operated terminals connected, via the access network, to the network providing the services, said system comprising

- connecting means (SL) for connecting the terminal to the network providing the services through an interface element (R1) linking the access network with the network providing the services, and

- means for generating the charging records (CDR) in response to the provision of access to the network providing the services,

c h a r a c t e r i z e d in that

- the system includes start-up means for generating a message indicating the start-up of the access service session for charging purposes when the user connects to the access network via the terminal,

- the system includes verification means (SLI) for generating verifiable charging records,

- the system includes checking means (WD) for checking the charging records generated, and

- the connecting means (SL) are responsive to the checking means (WD) for ~~connecting the terminal~~ to the network providing the services when the charging records are generated in an acceptable manner.

33. A system according to patent claim 32, c h a r a c t e r i z e d in that the means for generating the charging messages are incorporated into the terminal.

34. A system according to patent claim 32, c h a r a c t e r i z e d in that it also comprises identification means (CR) for identifying the subscriber associated with the current user of the terminal.

35. A system according to patent claim 33, c h a r a c t e r i z e d in that the identification elements (CR) are in connection with the terminals.

36. A system according to patent claim 32, c h a r a c t e r i z e d in that the checking means comprise at least one separate charging server (WD) to which several terminals send charging messages.

37. A system according to patent claim 32, c h a r a c t e r i z e d in that the connecting means include a separate server (SL) in the network, said server controlling a router (R1) serving as the interface element in accordance with the messages transmitted by the charging server.

38. A system according to patent claim 36, c h a r a c t e r i z e d in that the identification means include a smart card reader (CR) connected to the terminal and a smart card issued to the user containing at least the identifier of the subscriber associated with the user.

39. A system according to patent claim 32, in which IP packets are transmitted, c h a r a c t e r i z e d in that

- the system makes use of an IP level routing protocol that supports terminal mobility, according to which protocol the terminal performs a registration when connecting to the access network, and

- the service start-up means are responsive to the registration, whereby the start-up message is generated in response to the registration.

40. A system according to patent claim 39 with a mobile IP routing protocol, whereby the system includes at least one home agent and at least one foreign agent, c h a r a c t e r i z e d in that the service start-up means are incorporated in the foreign agent in the system.

41. A system according to patent claim 39, c h a r a c t e r i z e d in that the system includes at least one server (DHCP_S) which allocates addresses and with which the terminals register, and that the service start-up means are located on said server.

THIS PAGE BLA

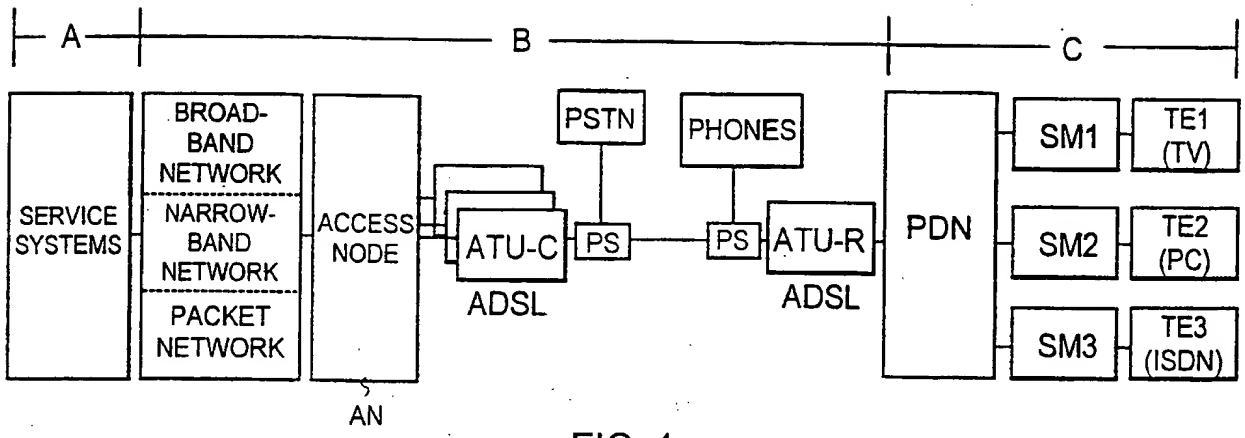

A
B
C
SERVICE SYSTEMS
BROAD-BAND NETWORK
NARROW-BAND NETWORK
PACKET NETWORK
ACCESS NODE
AN
ATU-C
ADSL
PS
PSTN
PS
PHONES
ATU-R
ADSL
PDN
SM1
SM2
SM3
TE1 (TV)
TE2 (PC)
TE3 (ISDN)

FIG. 1

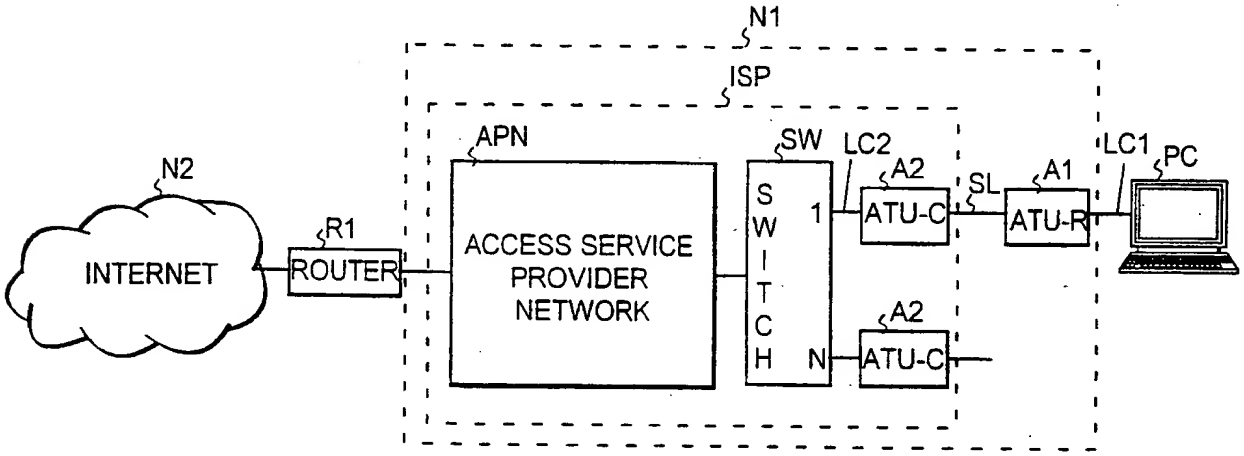

N1
ISP
APN
SW
LC2
A2
LC1
PC
N2
R1
INTERNET
ROUTER
ACCESS SERVICE PROVIDER NETWORK
SWITCH
1
N
ATU-C
SL
A1
ATU-R
A2
ATU-C

FIG. 2

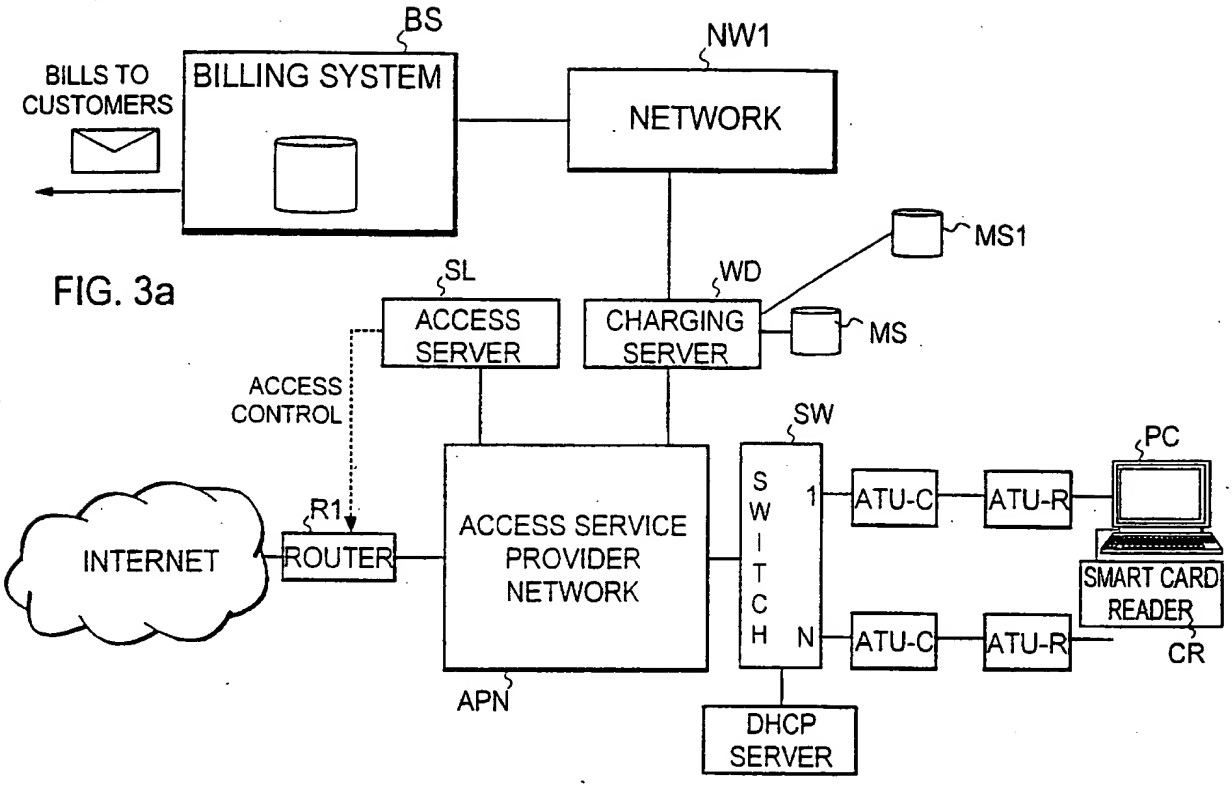

BS
BILLS TO CUSTOMERS
BILLING SYSTEM
NW1
NETWORK
MS1
SL
WD
ACCESS SERVER
CHARGING SERVER
MS
ACCESS CONTROL
SW
PC
R1
INTERNET
ROUTER
ACCESS SERVICE PROVIDER NETWORK
S W I T C H
1
N
ATU-C
ATU-R
SMART CARD READER
CR
APN
DHCP SERVER

FIG. 3a

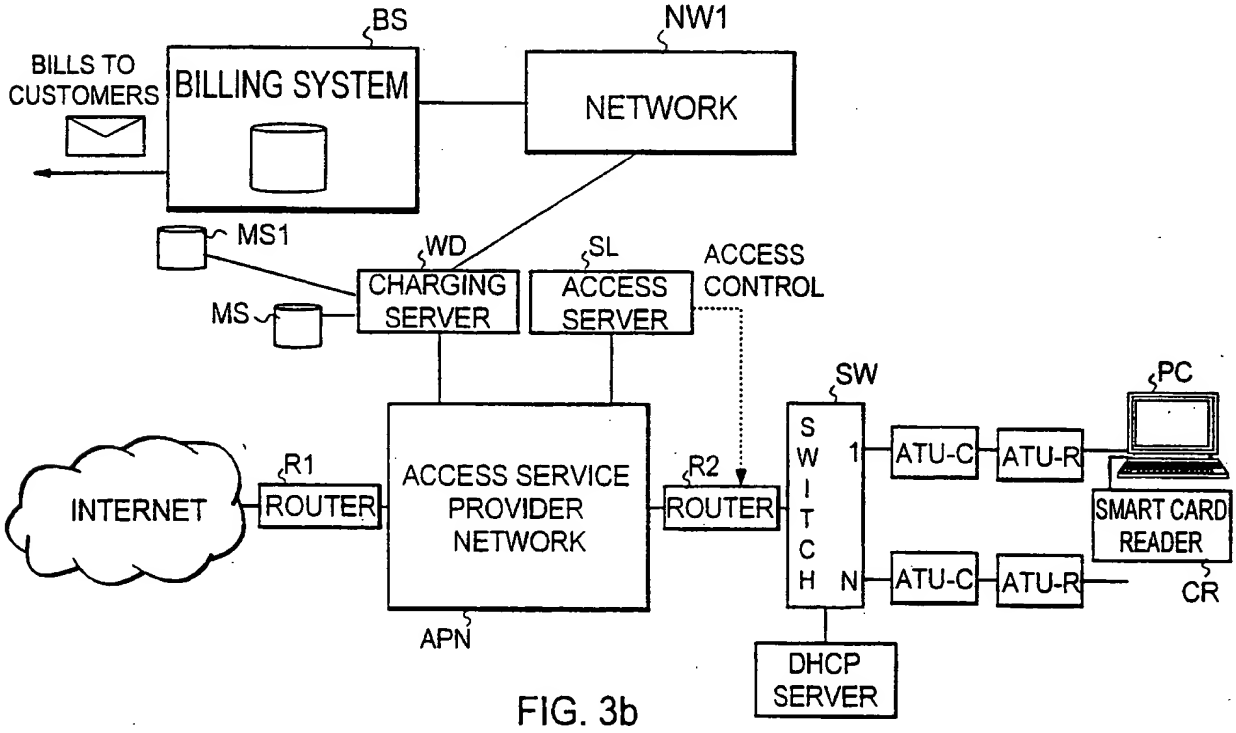

BS
BILLS TO CUSTOMERS
BILLING SYSTEM
NW1
NETWORK
MS1
WD
SL
ACCESS CONTROL
CHARGING SERVER
ACCESS SERVER
MS
SW
PC
R1
R2
INTERNET
ROUTER
ROUTER
ACCESS SERVICE PROVIDER NETWORK
S W I T C H
1
N
ATU-C
ATU-R
SMART CARD READER
CR
APN
DHCP SERVER

FIG. 3b

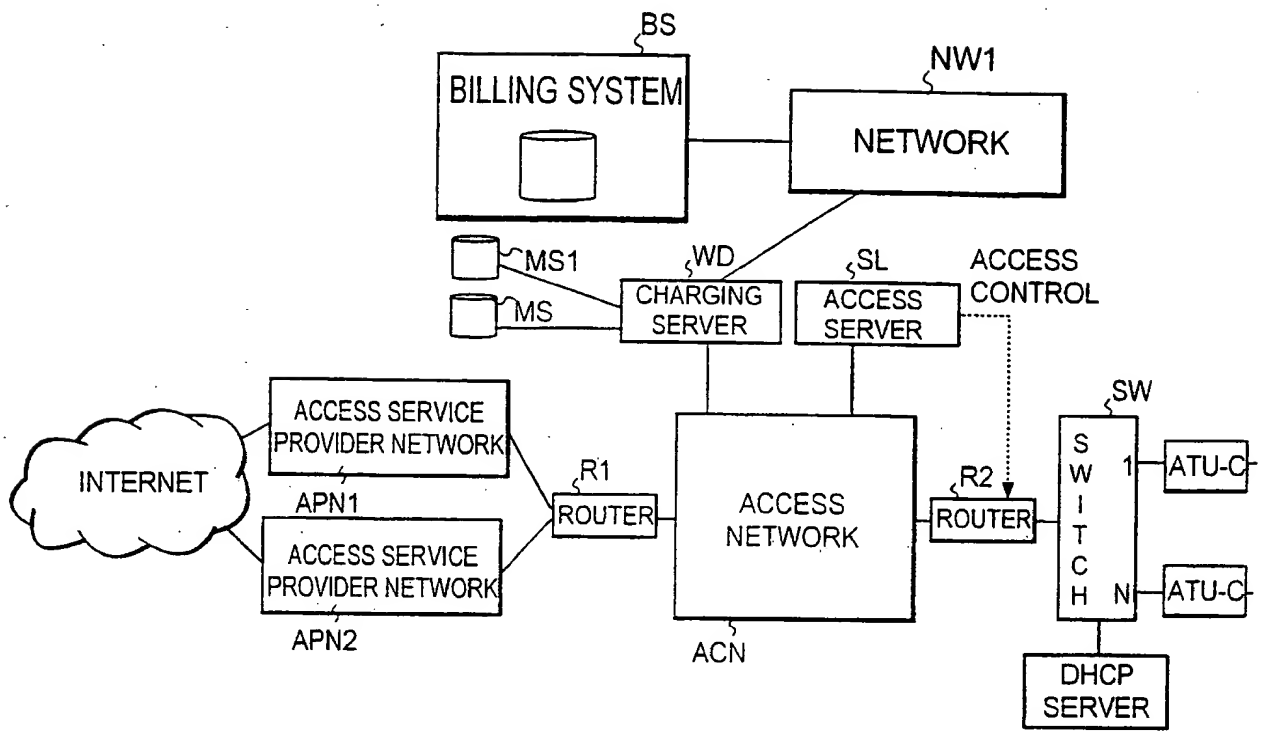

BS
BILLING SYSTEM
NW1
NETWORK
MS1
MS
WD
CHARGING SERVER
SL
ACCESS SERVER
ACCESS CONTROL
SW
INTERNET
ACCESS SERVICE PROVIDER NETWORK
APN1
ACCESS SERVICE PROVIDER NETWORK
APN2
R1
ROUTER
ACCESS NETWORK
ACN
R2
ROUTER
S W I T C H
1
N
ATU-C
ATU-C
DHCP SERVER

FIG. 3c

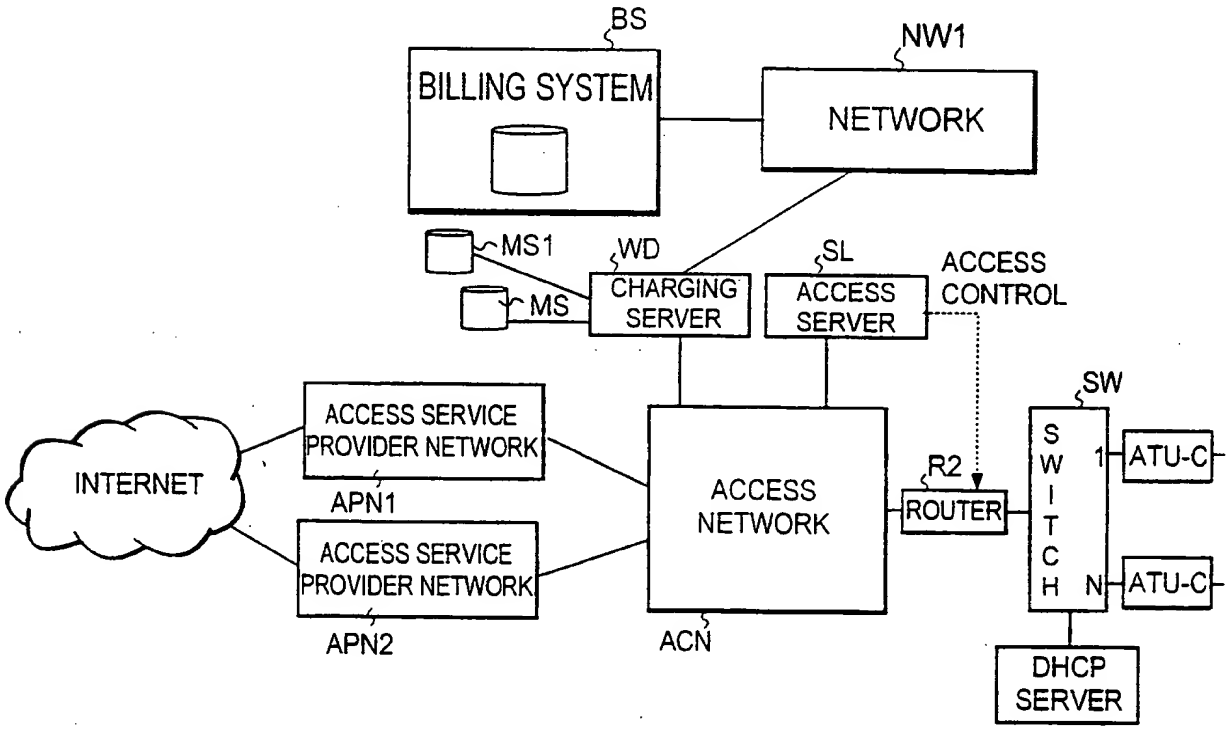

BS
BILLING SYSTEM
NW1
NETWORK
MS1
MS
WD
CHARGING SERVER
SL
ACCESS SERVER
ACCESS CONTROL
SW
INTERNET
ACCESS SERVICE PROVIDER NETWORK
APN1
ACCESS SERVICE PROVIDER NETWORK
APN2
ACCESS NETWORK
ACN
R2
ROUTER
S W I T C H
1
N
ATU-C
ATU-C
DHCP SERVER

FIG. 3d

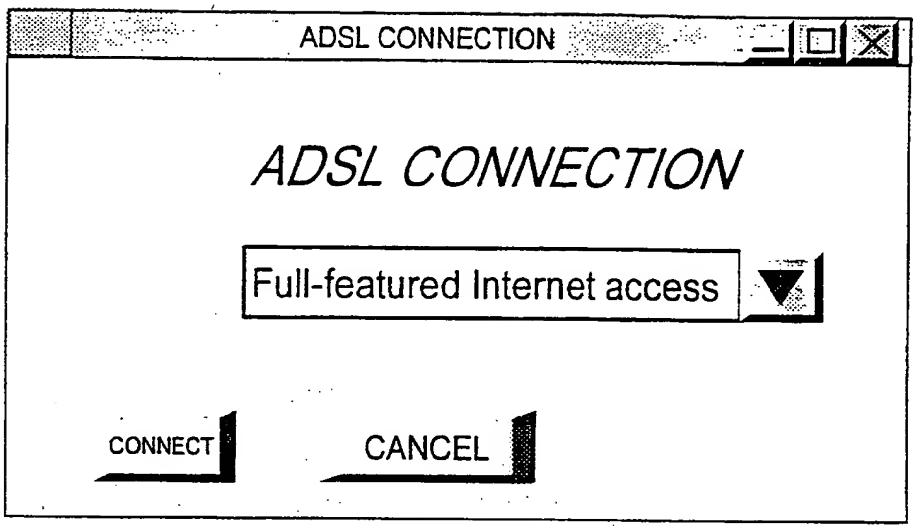

ADSL CONNECTION
ADSL CONNECTION
Full-featured Internet access
CONNECT
CANCEL

FIG. 4

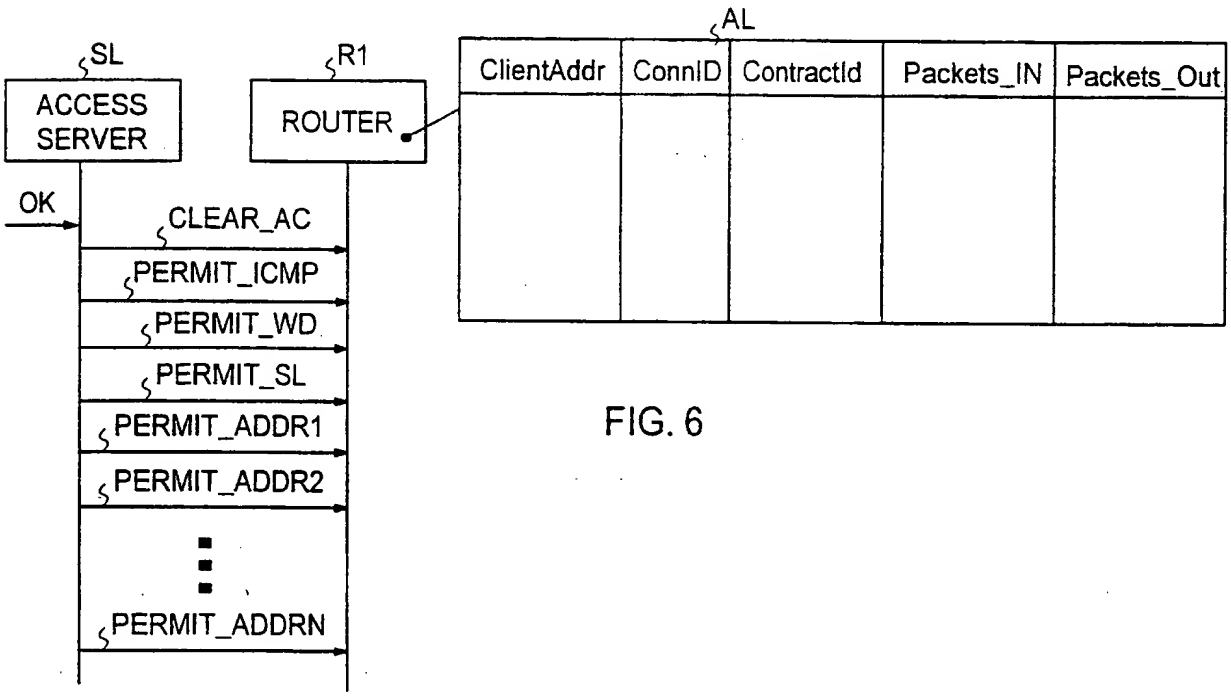

SL
ACCESS SERVER
R1
ROUTER
AL
ClientAddr
ConnID
ContractId
Packets_IN
Packets_Out
OK
CLEAR_AC
PERMIT_ICMP
PERMIT_WD
PERMIT_SL
PERMIT_ADDR1
PERMIT_ADDR2
PERMIT_ADDRN

FIG. 6

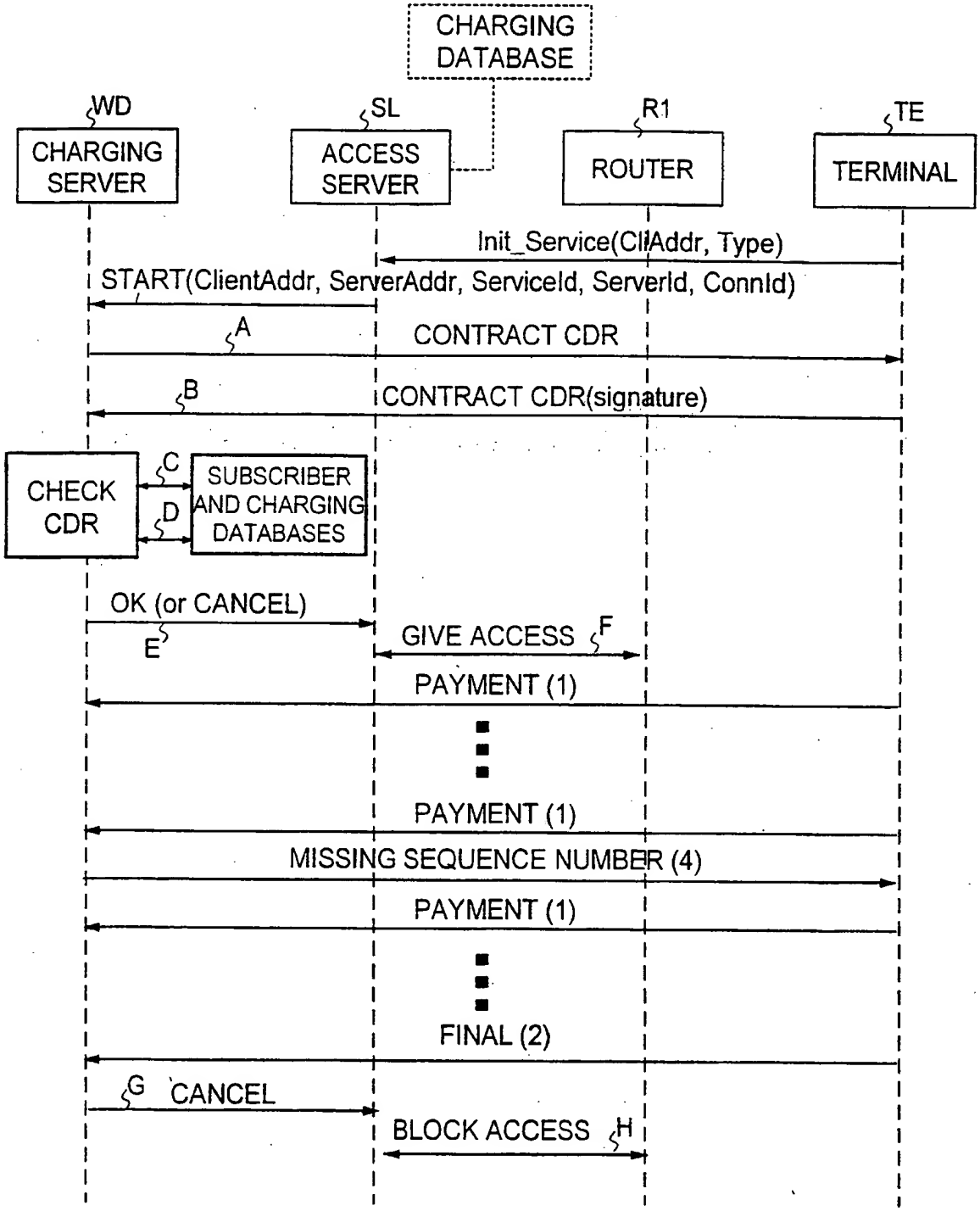

CHARGING DATABASE
WD
CHARGING SERVER
SL
ACCESS SERVER
R1
ROUTER
TE
TERMINAL
Init_Service(CliAddr, Type)
START(ClientAddr, ServerAddr, ServiceId, ServerId, ConnId)
A
CONTRACT CDR
B
CONTRACT CDR(signature)
CHECK CDR
C
D
SUBSCRIBER AND CHARGING DATABASES
OK (or CANCEL)
E
GIVE ACCESS
F
PAYMENT (1)
PAYMENT (1)
MISSING SEQUENCE NUMBER (4)
PAYMENT (1)
FINAL (2)
G
CANCEL
BLOCK ACCESS
H

FIG. 5

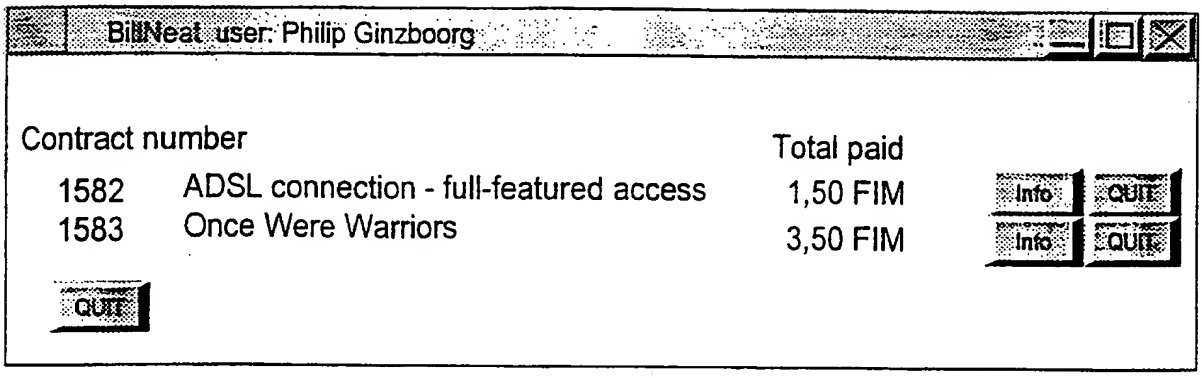


FIG. 7a

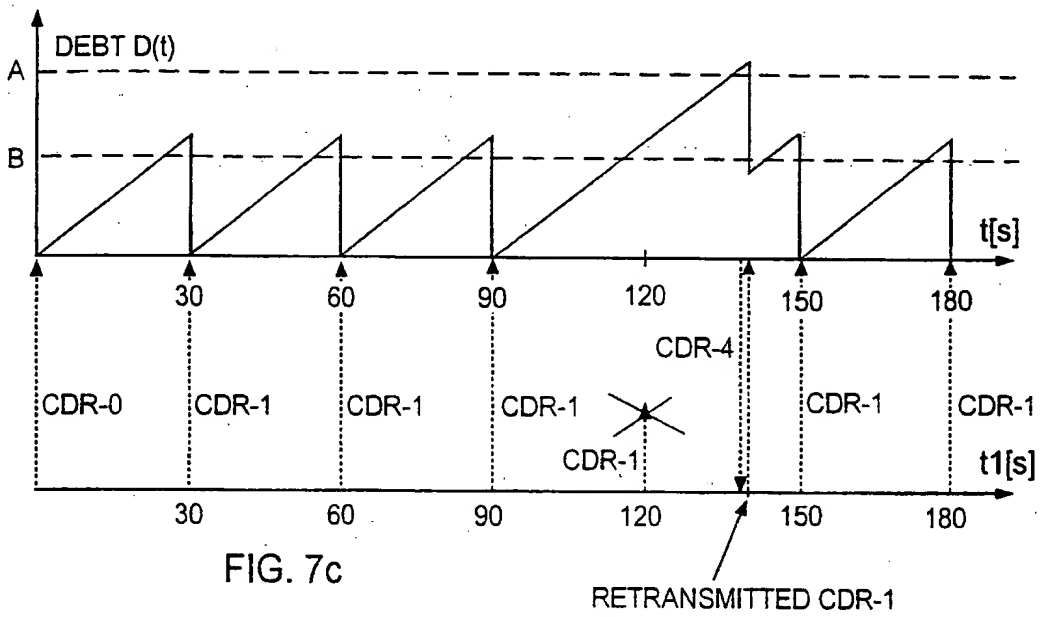


FIG. 7c

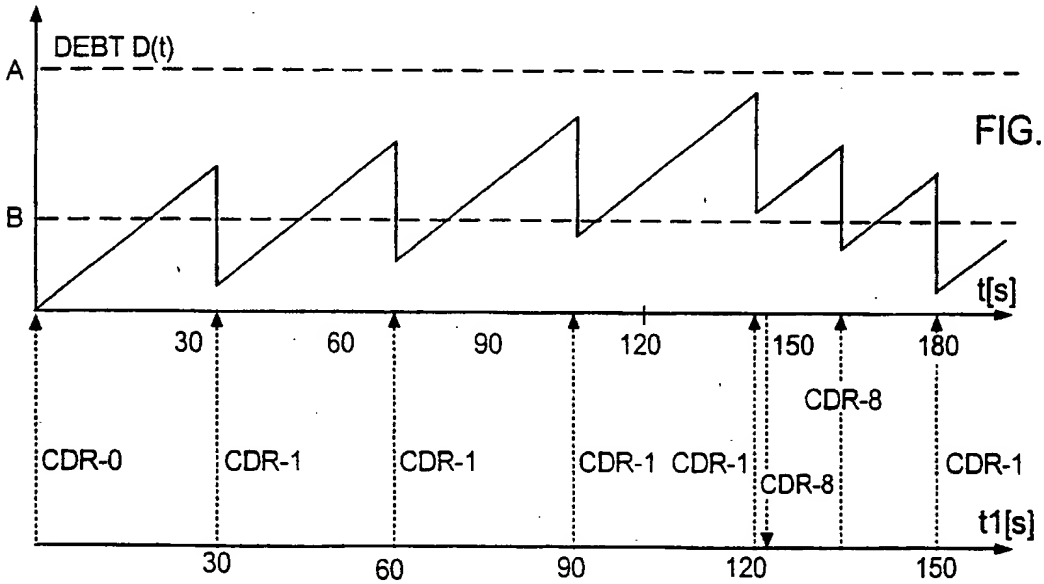


FIG. 7d

Name:	Philip Ginzboorg Itälahdenkatu 22 B 00210 Helsinki Finland	Billing server: Billing server ID: Billing date:	NRC Watchdog 1 423 3343 9730 24.6.1997
E-mail: Client ID:	philip.ginzboorg@research.nokia.com 711 5655 6654		

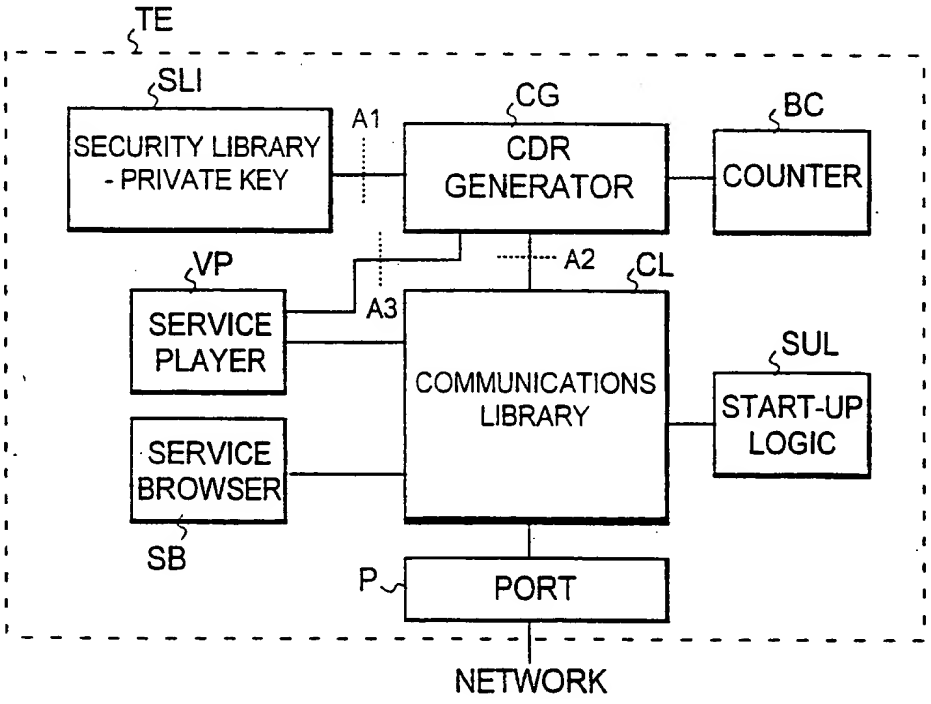
Billing period:	1.6.1997 - 15.6.1997
Period fee:	49,90 FIM
Service fee:	68,41 FIM
TOTAL:	118,31 FIM

Used services:

Service	Service type	Provider	Contract nr	Start time	Duration	PRICE
•	•	•	•	•	•	•
•	•	•	•	•	•	•
•	•	•	•	•	•	•

FIG. 7b

FIG. 9a



PAGE BLANK (USPTO)

FIG. 8

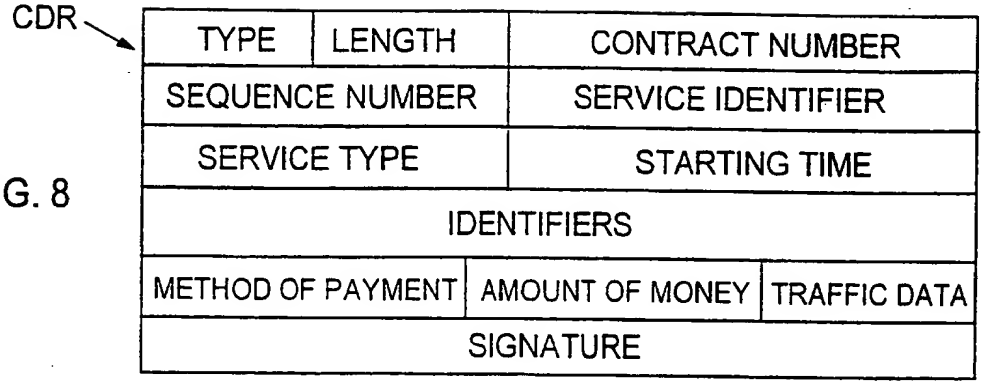


FIG. 9b

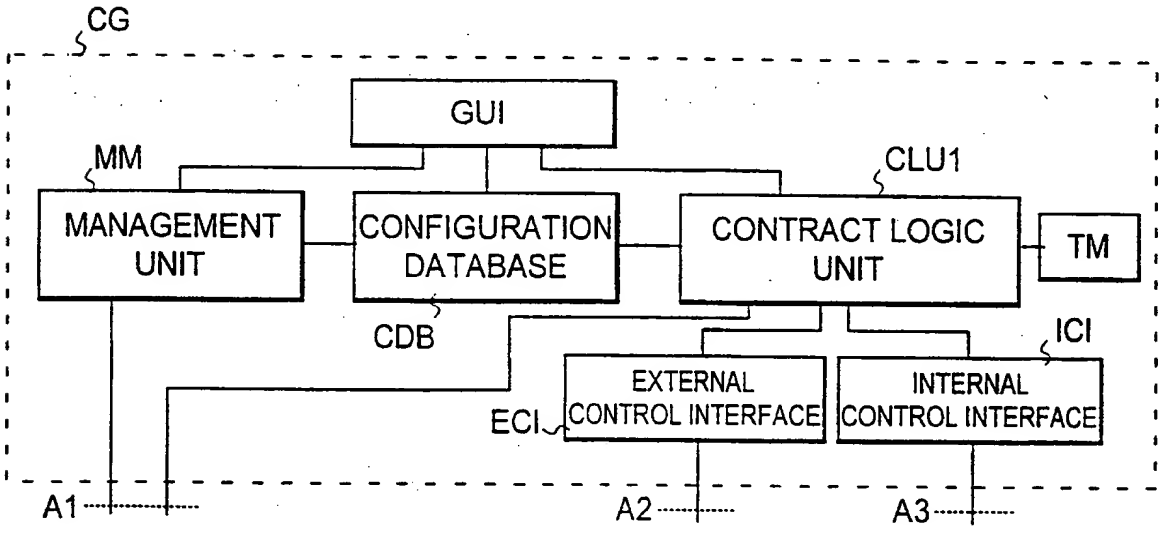
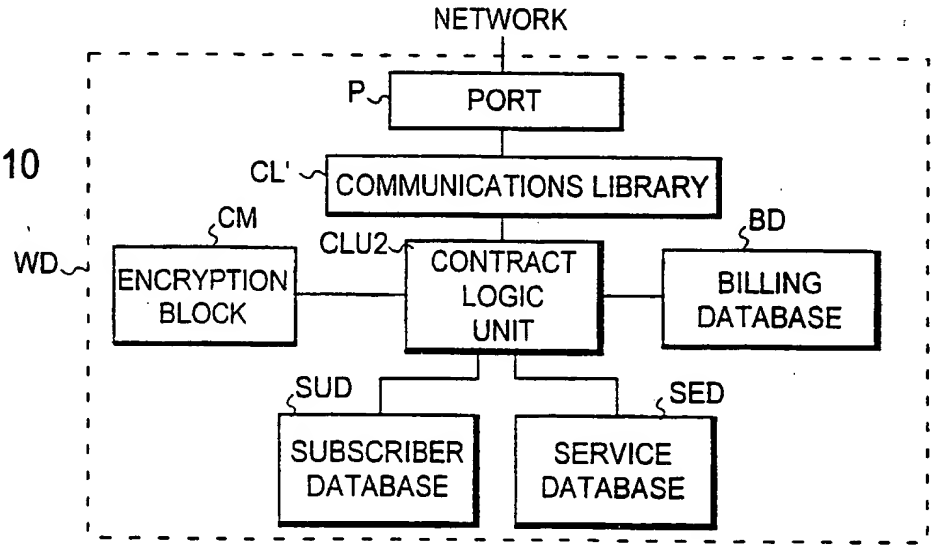


FIG. 10



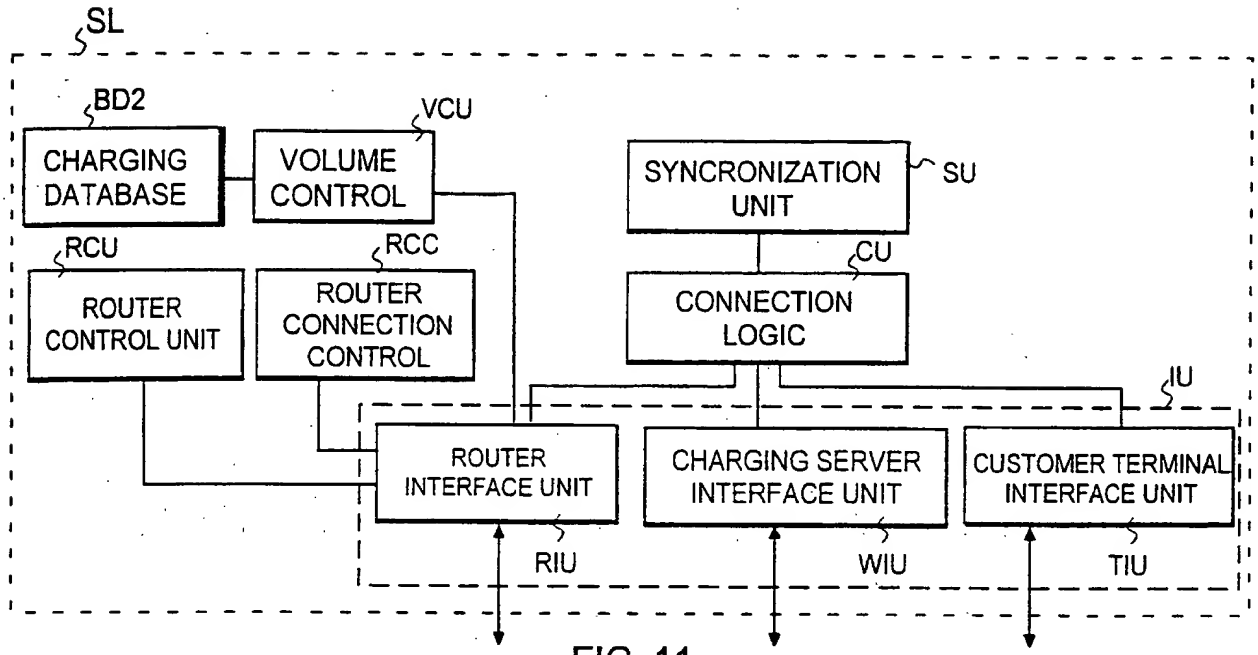
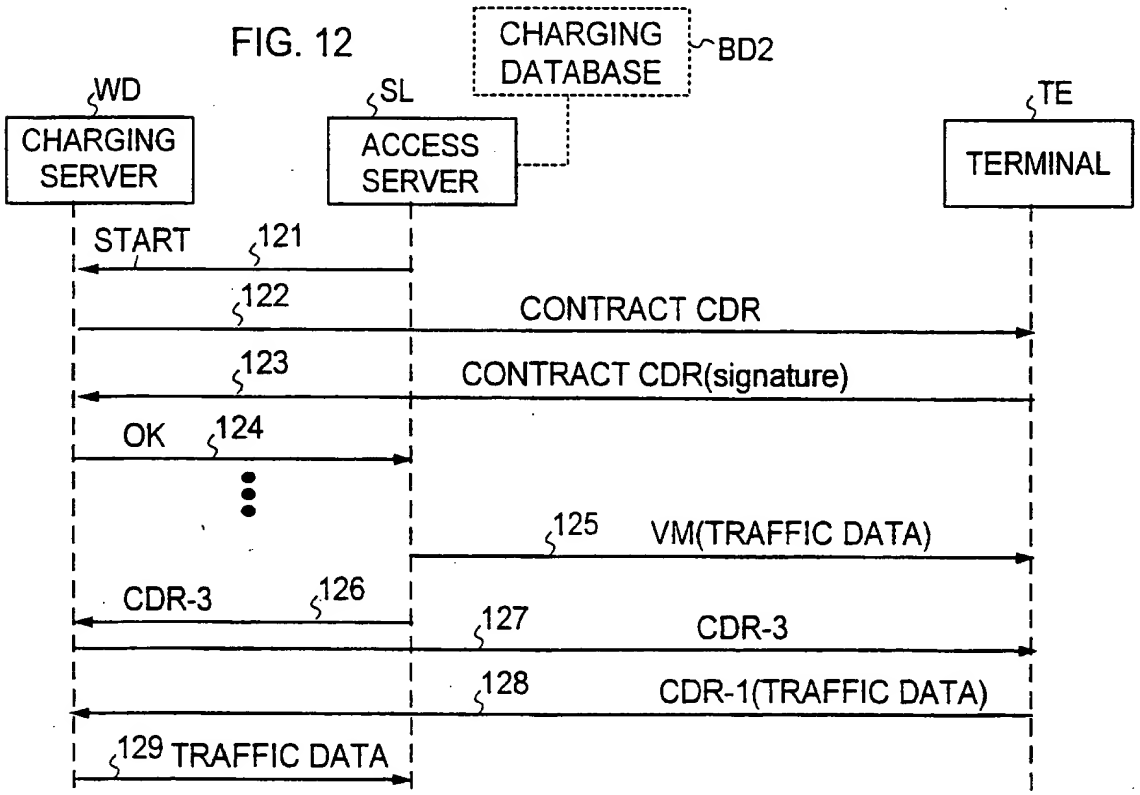

SL
BD2
CHARGING DATABASE
VCU
VOLUME CONTROL
SYNCRONIZATION UNIT
SU
RCU
ROUTER CONTROL UNIT
RCC
ROUTER CONNECTION CONTROL
CU
CONNECTION LOGIC
IU
ROUTER INTERFACE UNIT
CHARGING SERVER INTERFACE UNIT
CUSTOMER TERMINAL INTERFACE UNIT
RIU
WIU
TIU

FIG. 11

FIG. 12


CHARGING DATABASE
BD2
WD
CHARGING SERVER
SL
ACCESS SERVER
TE
TERMINAL
START
121
122
CONTRACT CDR
123
CONTRACT CDR(signature)
OK
124
125
VM(TRAFFIC DATA)
CDR-3
126
127
CDR-3
128
CDR-1(TRAFFIC DATA)
129 TRAFFIC DATA

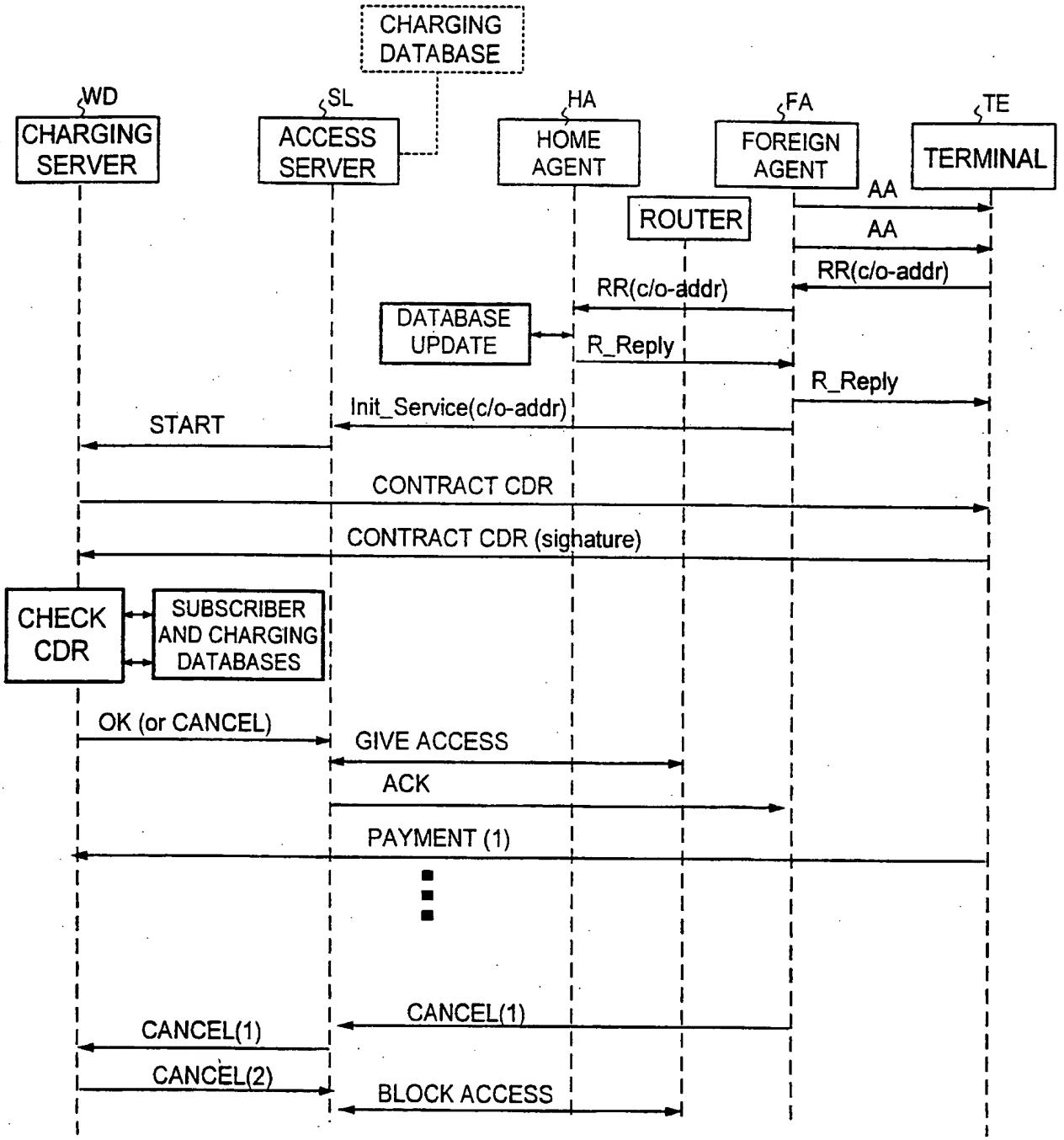

CHARGING DATABASE
WD
CHARGING SERVER
SL
ACCESS SERVER
HA
HOME AGENT
FA
FOREIGN AGENT
TE
TERMINAL
ROUTER
AA
AA
RR(c/o-addr)
RR(c/o-addr)
DATABASE UPDATE
R_Reply
R_Reply
Init_Service(c/o-addr)
START
CONTRACT CDR
CONTRACT CDR (sighature)
CHECK CDR
SUBSCRIBER AND CHARGING DATABASES
OK (or CANCEL)
GIVE ACCESS
ACK
PAYMENT (1)
CANCEL(1)
CANCEL(1)
CANCEL(2)
BLOCK ACCESS

FIG. 13

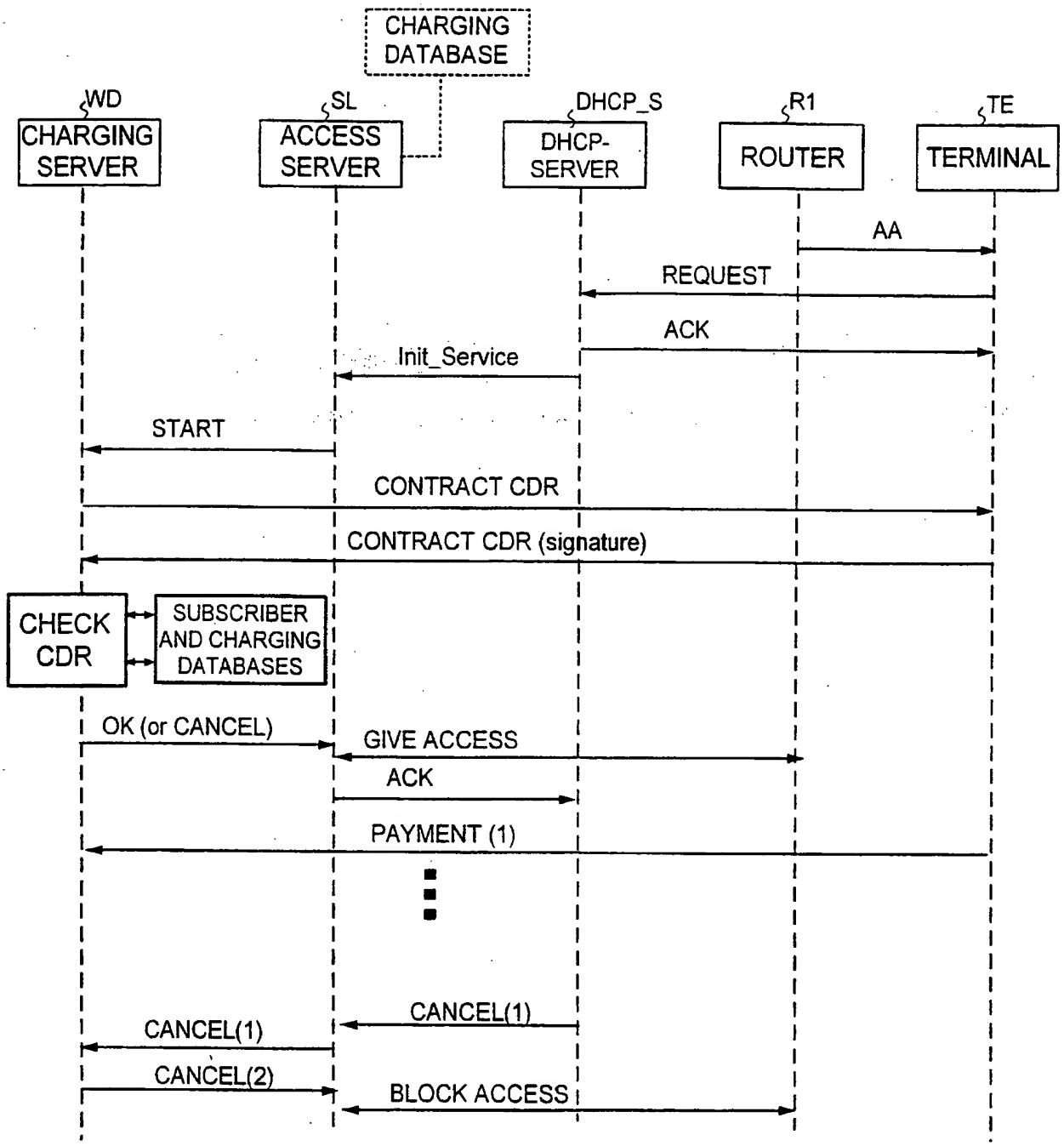

CHARGING DATABASE
WD
CHARGING SERVER
SL
ACCESS SERVER
DHCP_S
DHCP-SERVER
R1
ROUTER
TE
TERMINAL
AA
REQUEST
ACK
Init_Service
START
CONTRACT CDR
CONTRACT CDR (signature)
CHECK CDR
SUBSCRIBER AND CHARGING DATABASES
OK (or CANCEL)
GIVE ACCESS
ACK
PAYMENT (1)
CANCEL(1)
CANCEL(1)
CANCEL(2)
BLOCK ACCESS

FIG. 14

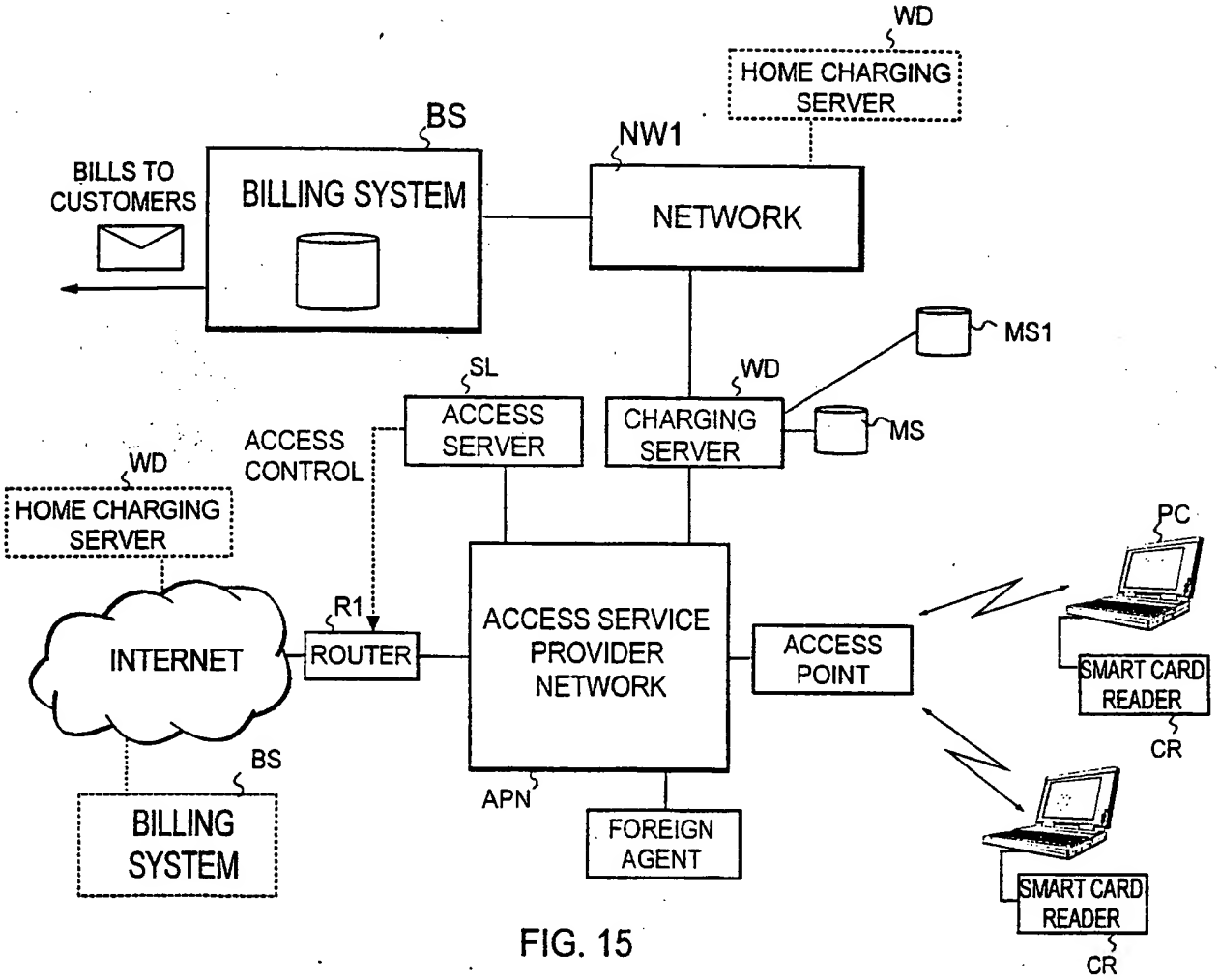

WD
HOME CHARGING SERVER
BS
NW1
BILLS TO CUSTOMERS
BILLING SYSTEM
NETWORK
MS1
SL
WD
ACCESS SERVER
CHARGING SERVER
MS
ACCESS CONTROL
WD
HOME CHARGING SERVER
PC
R1
INTERNET
ROUTER
ACCESS SERVICE PROVIDER NETWORK
ACCESS POINT
SMART CARD READER
CR
BS
BILLING SYSTEM
APN
FOREIGN AGENT
SMART CARD READER
CR

FIG. 15